QUANTUM

11 June 2025

SSL NETWORK EXTENDER (SNX)

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point SSL Network Extender (SNX) Administration Guide
For more about this release, see the home page.

Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

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

Revision History

Date	Description
11 June 2025	Updated: ■ *"Latest Available Versions of SNX" on page 16*
25 December 2024	Updated: ■ *" Getting Started with SSL Network Extender (SNX)" on page 13*
01 December 2024	Updated: ■ *"Introduction to SSL Network Extender (SNX)" on page 8* ■ *"Configuring an Advanced Native Application" on page 32* ■ *"SSL Network Extender (SNX) Versions and Requirements" on page 16*
07 March 2024	Added: ■ *"SSL Network Extender (SNX) Versions and Requirements" on page 16* Updated: ■ *"Downloading and Connecting the SNX Client for Linux or macOS" on page 74*
26 November 2023	First release of this document

Table of Contents

Introduction to SSL Network Extender (SNX)

SSL Network Extender is a thin client that remote users use to access internal resources that the administrator defines as applications.

SNX can work with the Mobile Access Software Blade or the IPsec VPN Software Blade.

The IPsec VPN Software Blade and the Mobile Access Software Blade require different licenses.

Workflow:

1. The administrator configures a Security Gateway as an SSL-enabled web server that supports Remote Access clients.
2. The remote user downloads the SNX client from the Security Gateway.
3. The remote user can access internal resources.

   In a Mobile Access Software Blade configuration, the remote user can access configured applications.

Comparison of SNX supported features with the Mobile Access Software Blade and the IPsec VPN Software Blade

Type of SNX	End User Experience	Supported Access Control Rules	Supported Operating Systems
SNX with Mobile Access Software Blade	The Mobile Access Portal downloads SNX from the Security Gateway automatically.	Supports Access Control rules in SmartConsole based on: ■ User groups ■ User roles ■ Networks ■ Subnets ■ IP addresses	■ Windows ■ Linux ■ macOS Supported only with Mobile Access Portal. CLI is not supported.

Type of SNX	End User Experience	Supported Access Control Rules	Supported Operating Systems
SNX with Remote Access VPN Software Blade	Users download SNX from a Security Gateway portal.	Supports Access Control rules in SmartConsole based on: ■ Networks ■ Subnets ■ IP addresses	■ Linux (CLI only) ■ macOS (CLI only) ■ Windows (IPsec VPN portal - works only with Internet Explorer)

If the Mobile Access Software Blade is enabled on the Security Gateway:

- SNX works through Mobile Access only.
- You must configure the Mobile Access policy:
  - Management Server R82 and higher:

    In SmartConsole > **Security Policies** view > section **Shared Policies** > section **Mobile Access** > click the page **Policy**.
  - Management Server R81.20 and lower:

    In SmartConsole > **Manage & Settings** view > click **Blades** > in the section **Mobile Access**, click **Configure in SmartDashboard** > tab **Mobile Access** > click the page **Policy**.

If the Mobile Access Software Blade is disabled and the IPsec VPN Software Blade is enabled on the Security Gateway:

- SNX works through the IPsec VPN Software Blade.
- You must configure the Access Control Policy in SmartConsole.

Important - If you configured the SSL Network Extender settings in the Security Gateway for the IPsec VPN Software Blade, and then you enabled the Mobile Access Software Blade, then you must reconfigure the required rules in the Mobile Access policy.The SSL Network Extender rules in the Access Control Policy do not apply anymore.

SNX Modes for Mobile Access Portal on an Endpoint Computer with Windows OS

SNX for Mobile Access supports **Network Mode** and **Application Mode**.

Category	Network Mode	Application Mode
Supported application types	All Native IP-based applications and web applications	Most Native IP-based applications and web applications are supported. OPSEC-certified applications are tested and verified UDP-based applications are not supported.
Supported web browsers on the client computer	■ Google Chrome ■ Mozilla Firefox ■ Microsoft Edge ■ Safari	■ Google Chrome ■ Mozilla Firefox ■ Microsoft Edge ■ Safari
Required privileges on the client computer	Administrator privileges required on the client computer	Administrator privileges not required on the client computer
How remote users open the application	Remote users can open applications in the Mobile Access portal or on the desktop of the endpoint computer.	Remote users can open applications only in the Mobile Access Portal. An application that is not supported in Application Mode does not appear in the Mobile Access Portal.

Note - Some Anti-Virus applications do not scan email when Microsoft Outlook is launched with SNX Application Mode because the mail is encrypted with SSL before the scanning begins.

Downloading SNX for Mobile Access or Remote Access VPN

Software Blade	Endpoint Computer Operating System	How to Download SNX
Mobile Access	Windows, Linux, or macOS	The endpoint computer automatically downloads SNX as a desktop application from the Mobile Access Portal.

Software Blade	Endpoint Computer Operating System	How to Download SNX
Remote Access VPN	Windows	The endpoint computer automatically downloads SNX as a desktop application from the Remote Access VPN portal.
Remote Access VPN	Linux or macOS	You must download SNX manually as a command line application. See *"Basic Configuration of SSL Network Extender for Remote Access VPN" on page 66*.

Commonly Used Concepts

These are commonly used concepts that you encounter when working with the SSL Network Extender:

Remote Access VPN

Refers to remote users accessing the network with client software such as Endpoint VPN clients, SSL clients, or third party IPsec clients.

The Security Gateway provides a *Remote Access VPN Service* to the remote clients.

Remote Access Community

A Remote Access Community, a Check Point concept, is a type of VPN community created specifically for users that usually work from remote locations, outside of the corporate LAN.

Office Mode

Office Mode is a Check Point remote access VPN solution feature. It enables a Security Gateway to assign a remote client an IP address.

This IP address is used only internally for secure encapsulated communication with the home network, and therefore is not visible in the public network.

The assignment takes place once the user connects and authenticates.

The assignment lease is renewed as long as the user is connected.

The address may be taken either from a general IP address pool, or from an IP address pool specified per user group, using a configuration file.

Visitor Mode

Visitor Mode is a Check Point remote access VPN solution feature. It enables tunneling of *all* Client-to-Security Gateway communication through a regular TCP connection on port **443**.

Visitor mode is designed as a solution for firewalls and Proxy servers that are configured to block IPsec connectivity.

Getting Started with SSL Network Extender (SNX)

Prerequisites and Known Limitations

Prerequisites for a Client Computer

The SSL Network Extender client-side prerequisites for remote clients are:

- A supported Windows, Linux, or macOS operating system.

  See *"SSL Network Extender (SNX) Versions and Requirements" on page 16*.

- A supported web browser.

  See *"SSL Network Extender (SNX) Versions and Requirements" on page 16*.

- In the SNX Network mode with the Mobile Access Software Blade, first-time client installation, uninstall, and upgrade require administrator privileges on the client computer.
- For the Remote Access VPN portal, you must allow ActiveX or Java Applet.

Prerequisites for a Security Gateway with the enabled Mobile Access Software Blade

- The specific Security Gateway must have a valid license for the SSL Network Extender.

Prerequisites for a Security Gateway with the enabled IPsec VPN Software Blade

- The specific Security Gateway must have a valid license for the SSL Network Extender.
- The specific Security Gateway must be configured as a member of the Remote Access Community, and configured to work with Visitor Mode.

  This does not interfere with Remote Access client functionality, but allows Remote Access client users to access internal resources with Visitor Mode.
- The same access rules are configured for Remote Access client and SSL Network Extender users.

Known Limitations for a ClusterXL Security Gateway Configuration

- Only ClusterXL Load Sharing mode is supported. High Availability mode is **not** supported.

- SNX connections do not survive cluster failover. Cluster failover may cause remote users to lose unsaved work. After cluster failover, remote users must reconnect.

Getting Started with SNX for the Mobile Access Software Blade

Procedure

1. See *"SSL Network Extender (SNX) Versions and Requirements" on page 16*.
2. Connect with SmartConsole to the Management Server that manages the Mobile Access Gateway.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click on the Security Gateway object.
5. In the left navigation tree, click **General Properties**.
6. On the **Network Security** tab, enable the Mobile Access Software Blade.

   See the *Mobile Access Administration Guide* for your version > "Getting Started with Mobile Access" section.
7. Configure the default SNX mode:
   a. In the navigation tree, click **Mobile Access** > **SSL Clients**.
   b. In the **SSL Network Extender Operation Mode** section, select the applicable option:
      - **Automatically decide on client time according to endpoint machine capabilities** (this is the default)
      - **Application Mode only**
      - **Network Mode only**

      For more information about SNX Application Mode and SNX Network Mode, see *"Introduction to SSL Network Extender (SNX)" on page 8*.
8. Click **OK**.
9. In the Mobile Access Policy, create a rule for at least one Native Application.

   See the *Mobile Access Administration Guide* for your version > "Mobile Access Authorization and Access Control" chapter.
10. Install the Access Control policy.

Getting Started with SNX for the IPsec VPN Software Blade

Procedure

1. See *"SSL Network Extender (SNX) Versions and Requirements" on the next page*.
2. Connect with SmartConsole to the Management Server that manages the Mobile Access Gateway.
3. From the left navigation panel, click **Gateways & Servers**.
4. Double-click on the Security Gateway object.
5. In the left navigation tree, click **General Properties**.
6. On the **Network Security** tab, enable the IPsec VPN Software Blade.

   See the *Remote Access VPN Administration Guide* for your version > chapter "Getting Started with Remote Access VPN" > section "Basic Security Gateway Configuration".
7. Enable SNX:
   a. In the navigation tree, click **VPN Clients**.
   b. In the **VPN clients allowed to connect to this gateway section**, select **Other** > **SSL Network Extender**.
8. Click **OK**.
9. In the Access Control policy, create the applicable rules.
10. Install the Access Control policy.

Important - If you configured the SSL Network Extender settings in the Security Gateway for the IPsec VPN Software Blade, and then you enabled the Mobile Access Software Blade, then you must reconfigure the required rules in the Mobile Access policy.The SSL Network Extender rules in the Access Control Policy do not apply anymore.

SSL Network Extender (SNX) Versions and Requirements

Latest Available Versions of SNX

Security Gateway Version	Jumbo Hotfix Accumulator Take	Latest Available SNX Version
R82	Quantum R82	**80008409**
R81.20	R81.20 Jumbo Hotfix Accumulator Take 79	**80008409**
R81.10	R81.10 Jumbo Hotfix Accumulator Take 152	**80008409**
R81	R81 Jumbo Hotfix Accumulator Take 89	**80008407**
R80.40	R80.40 Jumbo Hotfix Accumulator Take 211	**80008407**

How to Check the Version of SNX

To check the version of SNX installed on the Security Gateway:

Run this command on the Security Gateway in the Expert mode:

```
cat $CVPNDIR/htdocs/SNX/CSHELL/snx_ver.txt
```

To check the version of SNX installed on the endpoint computer:

Operating System	How to Check SNX Version
Windows	Open this file: `%Program Files (x86)%\CheckPoint\SSL Network Extender\ver.ini`
Linux and macOS	Run this CLI command: `snx -h`

Supported Operating Systems

SNX is supported for these operating systems:

SNX Version	Windows	macOS	Linux
80008407	■ Windows 11 ■ Windows 10 ■ Windows 8.1 ■ Windows 7 Ultimate, Enterprise, Professional, and Home	■ macOS 14 (Sonoma) ■ macOS 13 (Ventura) ■ macOS 12 (Monterrey) ■ macOS 11 (Big Sur) ■ macOS 10.15 (Catalina) ■ macOS 10.14 (Mojave) ■ macOS 10.13 (High Sierra)	■ Ubuntu 16.04 - 23.10 ■ CentOS 8 - 9 ■ RHEL 8 - 9.3 ■ Fedora 24 - 39 ■ openSUSE 42.1, 42.2, 42.3, Leap 15 - 15.5 For more information, see: sk119772 - Mobile Access Portal Agent Prerequisites for Linux.
80008304	■ Windows 11 ■ Windows 10 ■ Windows 8.1 ■ Windows 7 Ultimate, Enterprise, Professional, and Home	■ macOS 14 (Sonoma) ■ macOS 13 (Ventura) ■ macOS 12 (Monterrey) ■ macOS 11 (Big Sur) ■ macOS 10.15 (Catalina) ■ macOS 10.14 (Mojave) ■ macOS 10.13 (High Sierra)	■ Ubuntu 16.04 - 22.04 ■ CentOS 7.3 - 7.6 ■ RHEL 7.3 - 7.6 ■ Fedora 24 - 30 ■ openSUSE Leap 42.1, 42.2, 42.3, Leap 15, Leap 15.1 For more information, see: sk119772 - Mobile Access Portal Agent Prerequisites for Linux.

Supported Browsers

SNX is supported for these browsers:

Operating System	Microsoft Edge / Edge Chromium	Chrome	Firefox	Safari	Internet Explorer
Windows	✓	✓	✓	–	✓
Linux	–	✓	✓	–	–
macOS	–	✓	–	✓	–

Supported Java Versions

All endpoint computers must have Java installed.

Operating System	Supported Java Versions
Windows	▪ Oracle JRE version 8 ▪ Oracle JDK versions 11-20 ▪ OpenJDK versions 11-20
macOS	▪ Java Development Kit (JDK) version 8 ▪ Oracle JDK versions 11-19 ▪ OpenJDK versions 11-19
Linux	▪ Oracle JRE version 8 ▪ Oracle JDK version 11-19 ▪ OpenJDK versions 11-19

Additional Requirements for Linux

Linux endpoint computers must have specific tools and libraries installed:

- `certutil` (part of Mozilla NSS tools)
- `openssl`
- `xterm`

SSL Network Extender (SNX) Features

- Ability to run SNX from the command line on Linux and macOS (for the IPsec VPN Software Blade only).
- Easy installation and deployment.
- Intuitive and easy interface for configuration and use.
- The SNX mechanism is based on Visitor Mode and Office Mode.
- Automatic proxy detection is implemented.
- Small size client:

  Download size of the SNX client is smaller than 400,000 kilobytes.

  After the installation, the size of SNX is approximately 650,000 kilobytes
- All Security Gateway authentication schemes are supported:

  Authentication can be performed using a certificate, Check Point password or external user databases, such as SecurID, LDAP, RADIUS, and so forth (for the Mobile Access Software Blade only).

  Authentication for the IPsec VPN Software Blade: certificate and Check Point password.
- At the end of the session, no information about the user or Security Gateway remains on the client machine.
- Extensive logging capability, on the Security Gateway.
- SNX Upgrade is supported. SNX is upgraded in Jumbo Hotfix Accumulators.
- The SNX supports the RC4 encryption method.
- Users can authenticate using certificates issued by any trusted CA that is defined as such by the system administrator in SmartConsole.
- SNX can be configured to work in Hub Mode.

  VPN routing for remote access clients is enabled in Hub Mode.

  In Hub mode, all traffic is directed through a central Hub.

SSL Network Extender (SNX) for Mobile Access

Basic Configuration of SSL Network Extender for Mobile Access

Configuring a Simple Native Application

1. In SmartConsole, click **Objects > Object Explorer** (**Ctrl+E**).
2. Click **New Custom Application/Site > Mobile Application > Native Applications**.
3. Click **New**.

   The **Native Application** window opens.

General Properties

In the **General Properties** page, define the name of the Native Application.

Authorized Locations

1. Go to the **Authorized Locations** page.

   An authorized location ensures users of the Native Application can only access the specified locations using the specified services.
2. Fill in the fields:
   - **Host or Address Range** is the machine or address range on which the application is hosted.
   - **Service** is the port on which the machine hosting the application listens for communication from application clients.

Applications on the Endpoint Computer

1. Go to the **Endpoint Applications** page.
2. Fill in the fields:
   - **Add link in the Mobile Accessportal** must be selected if you want to make endpoint application(s) associated with the Native Applications available to users.

- **Link text** can include `$$user`, a variable that represents the user name of the currently logged-in user.
- **Tooltip** for additional information. Can include `$$user`, which represents the user name of the currently logged-in user.
- **Path and executable name** must specify one of these:
  - Full path of the application on the endpoint machines. For example: `c:\WINDOWS\system32\ftp.exe`
  - The location of the application by means of an environment variable.

    This allows the location of the application to be specified in a more generalized way.

    For example: `%windir%\system32\ftp.exe`
  - If the application is listed in the Windows **Start > Programs** menu, only the application name need be entered, as it appears to the user in the Start menu.

    For example **HyperTerminal**.
  - If the location of the application is in the `path` of the endpoint computer, only the application name need be entered.

    For example: `ftp.exe`

  Note - If the endpoint application is not available on the endpoint machine, the link to the application will not be shown in the end user's browser.
- **Parameters** are used to pass additional information to applications on the endpoint computer, and to configure the way they are launched.

Using the $$user Variable in Native Applications

You can use the "`$$user`" variable to define customized login parameters for native applications (in the **Parameters** field).

To do this, enter the `$$user` variable wherever you need to specify a user name.

For example, you can use the "`$$user`" variable to return the user name as a part of the login string for Remote Desktop.

In the parameter "`$$user.example.com`", the value resolves to the login string:

- For the username "Ethan", it resolves to: `ethan.example.com`
- For the username "Richard", it resolves to: `richard.example.com`

Completing the Native Application Configuration

To complete the configuration, add the Native application to a policy rule and install policy from SmartConsole.

If necessary, configure the Native Applications for Client-Based Access.

For Unified Access Policy, see the *Mobile Access Administration Guide* for your version > chapter "Mobile Access and the Unified Access Policy"

For legacy policy, see *Mobile Access Administration Guide* for your version > chapter "Getting Started with Mobile Access" > section "Sample Mobile Access Workflow".

Ensuring the Link Appears in the End-User Browser

If an endpoint application is defined by the administrator, but is not available on the endpoint machine, the link to the application does not appear in the Mobile Access Portal.

For example, the link does not appear:

- An endpoint application that is pre-installed on the endpoint machine (of type "Already Installed") is configured, and the application is not installed on the endpoint machine.
- A Downloaded-from-Gateway (Embedded) application requires Java, but Java is not installed on the endpoint machine.

Configuring SSL Network Extender as a VPN Client

To configure SSL Network Extender as a VPN client

1. From the **Gateways & Servers** tab, right-click the Mobile Access Security Gateway and select **Edit**.

   The Security Gateway properties window opens and shows the **General Properties** page.

2. From the navigation tree, click **Mobile Access > SSL Clients**.

   SSL Network Extender is automatically enabled when the Mobile Access Software Blade is enabled.

3. Select an option:

- **Automatically decide on client type according to endpoint machine capabilities** downloads the SSL Network Extender Network Mode client if the user on the endpoint machine has administrator permissions, and downloads the Application Mode client if the user does not have administrator permissions.
- **Application Mode only** specifies that the SSL Network Extender Application Mode client is downloaded to the endpoint machines - irrespective of the capabilities of the endpoint machine.
- **Network Mode only** specifies that the SSL Network Extender Network Mode client is downloaded to the endpoint machines - irrespective of the capabilities of the endpoint machine. The user on the endpoint machine must have administrator permissions in order to access Native Applications.

4. Click **OK**.
5. Install the Access Control policy.

   If you had SSL Network Extender configured through IPsec VPN and now you enabled the Mobile Access Software Blade on the Security Gateway, you must reconfigure the SSL Network Extender policy in the Mobile Access tab of SmartDashboard. Rules regarding SSL Network Extender in the main security rule base are not active if the Mobile Access tab is enabled.

Configuring Office Mode

When working with Office Mode, Remote Access clients receive an IP address allocated for them by the VPN administrator. These addresses are used by the clients in the source field of the IP packets they build. Since the IP packets are then encrypted and encapsulated, the packets appear to the Internet with their original IP address. To the organization's internal network, after decapsulation and decryption, they appear with the allocated IP address. The clients seem to be on the internal network.

For more about Office Mode, see the *Remote Access VPN Administration Guide* for your version.

Configure Office Mode in **Gateway Properties > Mobile Access > Office Mode**. The settings configured here apply to Mobile Access clients and IPsec VPN clients.

Office Mode Method

Choose the methods used to allocate IP addresses for Office Mode. All of the methods selected below will be tried sequentially until the office mode IP addresses are allocated.

- **From $FWDIR/conf/ipassignment.conf**

  You can over-ride the Office Mode settings created on Security Management Server. Edit the plain text file `ipassignment.conf` in the `$FWDIR/conf/` directory on the Check Point Security Gateway. The Security Gateway uses these Office Mode settings and not those defined for the object in Security Management Server.

The `ipassignment.conf` file can specify:

- An IP per user/group, so that a particular user or user group always receives the same Office Mode address. This allows the administrator to assign specific addresses to users, or particular IP ranges/networks to groups when they connect using Office Mode.
- A different WINS server for a particular user or group.
- A different DNS server.
- Different DNS domain suffixes for each entry in the file.

- **From the RADIUS server used to authenticate the user**

  A RADIUS server can be used for authenticating remote users. When a remote user connects to a Security Gateway, the user name and password are passed on to the RADIUS server, which checks that the information is correct, and authenticates the user.

- **Using one of the following methods**

  - **Manually (IP pool)**

    Create a Network Object with the relevant addresses. The allocated addresses can be illegal but they have to be routable within the internal network.

  - **Automatically (Using DHCP)**

    Specify the machine on which the DHCP server is installed. In addition, specify the virtual IP address to which the DHCP server replies. The DHCP server allocates addresses from the appropriate address range and relates to VPN as a DHCP relay agent. The virtual IP address must be routable to enable the DHCP send replies correctly.

    DHCP allocates IP addresses per MAC address. When VPN needs an Office Mode address, it creates a MAC address that represents the client and uses it in the address request. The MAC address can be unique per machine or per user. If it is unique per machine, then VPN ignores the user identity. If different users work from the same Remote Access client they are allocated the same IP address.

Multiple Interfaces

If the Security Gateway has multiple external interfaces, there might be a routing problem for packets whose destination address is a client working in Office Mode. The destination IP address is replaced when the packet is encapsulated and thus previous routing information becomes irrelevant. Resolve this problem by setting the Security Gateway to **Support connectivity enhancement for gateways with multiple external interfaces**. Do not select this option if your Security Gateway has only one external interface, as this operation affects the performance.

Anti-Spoofing

If this option is selected, VPN verifies that packets whose encapsulated IP address is an Office Mode IP address are indeed coming from an address of a client working in Office Mode.

If the addresses are allocated by a DHCP server, VPN must know the range of allocated addresses from the DHCP scope for the Anti-Spoofing feature to work. Define a Network object that represents the DHCP scope and select it here.

IP Pool Optional Parameters

Configure additional optional parameters for how office mode addresses are assigned by clicking **Optional Parameters**. If the office mode addresses are allocated from an IP pool, this window allows you to you specify the DNS and WINS addresses by selecting the appropriate Network Objects. In addition, specify the backup DNS and WINS servers and supply the Domain name.

If the office mode addresses are allocated by a DHCP server, DNS and WINS addresses are set on the DHCP server.

These details are transferred to the Remote Access client when a VPN is established.

IP Lease Duration

Specify the amount of time after which the Remote Access client stops using the allocated IP address and disconnects. By default, the duration is 15 minutes. The client tries to renew the IP address by requesting the same address after half of the set time has elapsed. When this request is granted, the client receives the same address until the lease expires. When the new lease expires, it must be renewed again.

Configuring SSL Network Extender Advanced Options

To configure SSL Network Extender advanced options:

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Additional Settings > VPN Clients**.
3. From the **Advanced Settings for SSL Network Extender section**, click **Edit**.
4. Configure the applicable options.
5. Click **OK**.
6. Click **Save**.
7. Close SmartDashboard.
8. In SmartConsole, install the Access Control policy.

Deployment Options

- **Client upgrade upon connection**

  Specifies how to deploy a new version of the SSL Network Extender Network Mode client on endpoint machines, when it becomes available.

  Note - Upgrading requires Administrator privileges on the endpoint machine.

- **Client uninstall upon disconnection**

  Specifies how to handle the installed SSL Network Extender Network Mode client on the endpoint machine when the client disconnects.

  - **Do not uninstall** - Allows the user to manually uninstall if they wish to.
  - **Ask User** - Allows the user to choose whether or not to uninstall.
  - **Always uninstall** - Does so automatically, when the user disconnects.

Encryption

- **Supported Encryption methods**

  Configures the strength of the encryption used for communication between SSL Network Extender clients and all Mobile Access Security Gateways and Clusters that are managed by the Security Management Server.

  - **AES, 3DES**

    This is the default setting. The 3DES encryption algorithm encrypts data three times, for an overall key length of 192 bits.

  - **AES, 3DES or RC4**

    Configures the SSL Network Extender client to support the RC4 encryption method, as well as AES and 3DES. RC4 is a variable key-size stream cipher. The algorithm is based on the use of a random permutation. It requires a secure exchange of a shared key that is outside the specification. RC4 is a faster encryption method than 3DES.

Launch SSL Network Extender Client

These settings define the behavior of the SSL Network Extender clients when launched on the endpoint machines.

- **On demand, when user clicks 'Connect" on the portal**

  SSL Network Extender only opens when the user clicks "Connect" from the Mobile Access Portal.

- **Automatically, when user logs on**

  When users log in to the Mobile Access Portal, SSL Network Extender launches automatically.

- **Automatically minimize client window after client connects**

  For either of the options above, choose to minimize the SSL Network Extender window to the system tray on the taskbar after connecting. This provides better usability for non-technical users.

Endpoint Native Applications

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.

SSL Network Extender automatically works with Mobile Access to support native applications.

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.

A native application is defined by the:

- Server hosting applications.
- Services used by applications.
- Connection direction (usually client to server, but can also be server to client, or client to client).
- Applications on the endpoint (client) machines.

  These applications are launched on demand on the user machine when the user clicks a link in the user portal.

  They can be one of these:

  - Already installed on the endpoint machine
  - Run via a default browser
  - Downloaded-from-Mobile Access

When defining a Native Application, you can define applications on endpoint machines. These applications launch on the endpoint machine when the user clicks a link in the Mobile Access Portal. You do not have to configure endpoint applications for users using SSL Network Extender in Network Mode, as they will be able to access them using their native clients.

Application Installed on Endpoint Machine

These endpoint applications are already installed on the endpoint machines.

Application Runs Via a Default Browser

Run via default browser is used to define a link to any URL. The link appears in the Mobile Access Portal, and launches the current Web browser (the same browser as the Mobile Access Portal). The link can include $$user, which represents the user name of the currently logged-in user.

This option has a user experience similar to a Web Application with a URL: The application is opened in a Web browser. However, Mobile Access Web applications perform Link Translation on the URL and encrypt the connection over SSL, while the "Run via default browser" option with SSL Network Extender does not perform link translation, and encrypts using SSL Network Extender. You may prefer to define a Native Application rather than a Web Application for convenience, or because some websites have problems working with Link Translation.

Applications Downloaded-from-Gateway

Downloaded-from-Gateway applications let you select applications that download from Mobile Access to the endpoint computer when the user clicks a link in the Mobile Access Portal. The list of available applications depends on the version of the Security Gateway.

These applications allow end users to securely use client-server applications, without requiring a native client to be installed on their machines.

Mobile Access has built-in applications that the administrator can configure. Downloaded-from-Gateway applications are either Java-based applications or single-executable applications (including batch files). All the applications that are available by default, other than the Terminal (PuTTY) client, are Java based applications, and are therefore multi-platform applications. The PuTTY client can only be used on Windows machines.

You can add Native Applications for Client-Based Access, in addition to the built-in applications.

The Downloaded-from-Gateway applications are third-party applications, which are supplied as-is, and for which Check Point provides limited support.

Some of these packages are not signed by Check Point, and when they are downloaded by end- users a popup warning informs the user that the package is not signed.

Downloaded-from-Gateway Applications

Application	Description
Remote Desktop (RDP)	Downloaded-from-Gateway Client for Windows NT Terminal Server and Windows 2000/2003 Terminal Services. Communicates using Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required. Runs on Java 1.1 up (optimized for 1.4), and works on Linux, Windows and Mac.
Terminal (PuTTY)	An implementation of Telnet and SSH for Win32 platforms, including an Xterm terminal emulator.
Jabber	Downloaded-from-Gateway Jabber Client is an instant messenger based on the Jabber protocol. Runs on every computer with at least Java 1.4.
FTP	Graphical Java network and file transfer client. Supports FTP using its own FTP API and various other protocols like SMB, SFTP, NFS, HTTP, and file I/O using third party APIs, includes many advanced features such as recursive directory up/download, browsing FTP servers while transferring files, FTP resuming and queuing, browsing the LAN for Windows shares, and more.
Telnet	Telnet terminal. Provides user oriented command line login sessions between hosts on the Internet.
SSH	Secure Shell (SSH) is designed for logging into and executing commands on a networked computer. It provides secure encrypted communications between two hosts over an insecure network. An SSH server, by default, listens on the standard TCP port 22.
TN3270	IBM 3270 terminal emulator tailored to writing screen-scraping applications. TN3270 is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminal.
TN5250	IBM 5250 terminal emulator that interprets and displays 5250 data streams.

Notes:

- You can also use Native Applications for Client-Based Access.
- When users are connected to the Mobile Access Gateway with SSL Network Extender in Application Mode, the Downloaded-from-Gateway applications do not work inside Endpoint Security On Demand Secure Workspace.

Configuring Authorized Locations per User Group

The authorized locations (hosts or address ranges) of a Native application are defined in the **Authorized Locations** page of the Native Application. However, it is also possible to configure authorized locations per user group. Users who belong to two or more groups can access the union of the authorized locations of the groups.

For configuration details, see sk32111.

Configuring an Advanced Native Application

Overview

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.

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.

A native application is defined by the:

- Server hosting applications.
- Services used by applications.
- Connection direction (usually client to server, but can also be server to client, or client to client).
- Applications on the endpoint (client) machines. These applications are launched on demand on the user machine when the user clicks a link in the user portal. They can be:
  - Already installed on the endpoint machine, or
  - Run via a default browser, or
  - Downloaded from Mobile Access.

In SmartConsole R82 and higher, you can see the Native Applications in the **Objects** menu > **Object Explorer** > **Applications/Categories** > **Custom Applications/Categories** > **Mobile Applications**.

In SmartConsole R81.20 and lower, you can see the Native Applications in SmartDashboard > **Applications** > **Native Applications**.

Workflow

1. Create a new Native Application.

   Steps on a Management Server R82 and higher

   a. In SmartConsole, in the top right corner, click the **Objects** panel.

   b. Click **New** > **More** > **Custom Application/Site** > **Mobile Application** > **Native Application**.

      The **Native Application** window opens.

Steps on a Management Server R81.20 and lower

a. In SmartConsole, from the left navigation panel, click **Manage & Settings**.

b. In the top left panel, click **Blades**.

c. In the **Mobile Access** section, click **Configure in SmartDashboard**.

SmartDashboard opens and shows the **Mobile Access** tab.

d. From the left navigation tree, click **Applications** > **Native Applications**.

e. Click **New**.

The **Native Application** window opens.

2. Configure the new Native Application.

a. In the **Name** field, enter the name for this object.

b. **Optional:** In the **Comment** field, enter the applicable text.

c. Follow the corresponding procedures below:

- *"Configuring Connection Direction" on the next page*
- *"Configuring Multiple Hosts and Services" on page 35*
- *"Configuring the Endpoint Application to Run Via a Default Browser" on page 36*
- *"Configuring Automatic Start of the Application" on page 37*
- *"Making a Native Application Available in the Application Mode" on page 38*
- *"Configuring Automatic Run of Commands or Scripts" on page 39*

In addition, see *"Protection Levels for Native Applications" on page 42*.

d. Click **OK** to close the new Native Application object.

3. Add the Native Application to the Mobile Access Policy

Steps on a Management Server R82 and higher

a. From the left navigation panel, click **Security Policies**.

b. In the **Shared Policies** section, in the **Mobile Access** section, click **Policy**.

c. Add the Native Application object to the applicable Mobile Access Policy rule.

Steps on a Management Server R81.20 and lower

a. In SmartDashboard, from the left navigation tree, click **Policy**.

b. Add the Native Application object to the applicable Mobile Access Policy rule.

c. Save the changes in SmartDashboard.

d. Close SmartDashboard.

4. In SmartConsole, install the Access Control Policy.

Configuring Connection Direction

Procedure

1. Create a new Native Application or edit an existing Native Application.
2. On the **General Properties** page, in the **Advanced** section, click **Connection direction**.
3. In the **Direction of communication from the connection initiator** section, in the **Connection direction** field, select the applicable option:
   - **Client to server**

     This is the default option.

     When you create a client to server application and assign it to a user group, you enable users of the group to initiate a connection to the specified server.

     Example: Telnet.
   - **Server to client**

     When you create a server to client application, the specified server can initiate a connection to all SSL Network Extender or Secure Client Mobile users currently logged on to the Mobile AccessSecurity Gateway, regardless of their group association.

     Example: X11.
   - **Client to client**

     When you create a client to client Native Application and assign it to a user group, you enable users of that group to initiate a connection to all of the SSL Network Extender or Secure Client Mobile users currently logged on to Mobile Access, regardless of their user group association.

     Example: Running Remote Administration from one client to another.

     Note - A "Client to client" Native Application does not require configuration of a destination address.
4. Click **OK** to close the new **Advanced** window.
5. Click **OK** to close the new Native Application object.

Configuring Multiple Hosts and Services

The Native Application can reside on a range of hosts, which can be accessed by the native application clients. You can also specify more than one service that clients may use to communicate with the application.

Users of the native application can only access the specified locations using the specified services.

An authorized location ensures users of the Native Application can only access the specified locations using the specified services.

Procedure

1. Create a new Native Application or edit an existing Native Application.
2. On the **Authorized Locations** page, select the applicable option.
   - If you selected **Simple**:

     This option allows you to select one object in each field.

     - In the **Host/Address Range/Group** field, select the applicable object (a Host, a Network Group, or an Address Range object), to which the Native Application requires access.
     - In the **Service** field, select the applicable Service object (or Service Group object) to configure ports, on which the hosted application listens for communication from application clients.
   - If you selected **Advanced**:

     This option allows you to select multiple server objects and multiple service objects. For example, it may not be possible to group the required hosts or services into a single Network Group object or Services Group objects.

     a. Click **Edit**.

        The **Native Application Hosts** window opens.

     b. In the **Hosts** panel, select the applicable objects (Host, Network Group, and Address Range objects).

     c. In the **Services** panel, select the applicable objects (Service, or Service Group objects).

     d. Click **OK** to close the **Native Application Hosts** window.

     e. Click **OK** to close the **Native Application - Advanced** window.
3. Click **OK** to close the new Native Application object.

Configuring the Endpoint Application to Run Via a Default Browser

Procedure

1. Create a new Native Application or edit an existing Native Application.
2. On the **Endpoint Applications** page, select **Add a link to the applicable in the Mobile Access portal**.
3. Select **Advanced**.
4. Click **Edit**.

   The **Endpoint Applications - Advanced** window opens.
5. Click **Add**.

   The **Edit Endpoint Application** window opens.
6. Select **Run via default browser**.

   This is used to define a link to any URL. The link appears in the Mobile Access Portal, and launches the current Web browser (the same browser as the Mobile Access Portal). The link can include `$$user`, which represents the user name of the currently logged-in user.

   This option has a similar user experience to a Web Application with a URL: The application is opened in a Web browser. However, Mobile Access Web applications perform Link Translation on the URL and encrypt the connection over SSL, while the "Run via default browser" option with SSL Network Extender does not perform link translation, and encrypts using SSL Network Extender. You may prefer to define a Native Application rather than a Web Application for convenience, or because some Web sites have problems working with Link Translation.
7. Click **OK** to close the **Edit Endpoint Application** window.
8. Click **OK** to close the **Endpoint Applications - Advanced** window.
9. Click **OK** to close the new Native Application object.

Configuring Automatic Start of the Application

Procedure

1. Create a new Native Application or edit an existing Native Application.
2. On the **Endpoint Applications** page, select **Add a link to the applicable in the Mobile Access portal**.
3. Select **Advanced**.
4. Click **Edit**.

   The **Endpoint Applications - Advanced** window opens.
5. Click **Add**.

   The **Edit Endpoint Application** window opens.
6. At the bottom of this page, click **Advanced**.
7. In the **Automatically Start this Application** section, select the applicable options:
   - **When SSL Network Extender is launched**

     Configures a Native Application to run a program or command automatically, after connecting to SSL Network Extender (either Network Mode or Application Mode).

     When more than one Native Application is defined for automatic connection, the applications run in the alphabetical order of the names of the Native Applications.
   - **When SSL Network Extender is disconnected**

     Configures a Native Application to run a program or command automatically, after disconnecting from SSL Network Extender (either Network Mode or Application Mode).

     When more than one Native Application is defined for automatic connection disconnection, the applications run in the alphabetical order of the names of the Native Applications.

     Note - Do **not** select this option to launch applications that require connectivity to the organization in the SNX Application Mode. In the SNX Network Mode, automatic start of applications when SSL Network Extender is disconnected, works correctly.
8. Click **OK** to close the **Advanced** window.
9. Click **OK** to close the **Edit Endpoint Application** window.
10. Click **OK** to close the **Endpoint Applications - Advanced** window.

11. Click **OK** to close the new Native Application object.

Making a Native Application Available in the Application Mode

Procedure

1. Create a new Native Application or edit an existing Native Application.
2. On the **Endpoint Applications** page, select **Add a link to the applicable in the Mobile Access portal**.
3. Select **Advanced**.
4. Click **Edit**.

   The **Endpoint Applications - Advanced** window opens.
5. Click **Add**.

   The **Edit Endpoint Application** window opens.
6. At the bottom of this page, click **Advanced**.
7. In the **SSL Network Extender Application Mode Compatibility** section, select **This endpoint application is supported when using SSL Network Extender in Application Mode**.

   This option make an application available to Application Mode clients. Users that connect using the SSL Network Extender Application Mode client are able to see a link to the application and launch it.

   Important:
   - Use this option if the application works well in Application Mode.
   - If you do **not** select this option, then users who connect with Application Mode, do not see it in their list of applications.
8. Click **OK** to close the **Advanced** window.
9. Click **OK** to close the **Edit Endpoint Application** window.
10. Click **OK** to close the **Endpoint Applications - Advanced** window.
11. Click **OK** to close the new Native Application object.

Configuring Automatic Run of Commands or Scripts

It is possible to configure a Native Application to run a program or command automatically, after connecting to or disconnecting from SSL Network Extender (either Network mode or Application mode).

Notes:

- The user must have the appropriate privileges on the endpoint machine to run the commands.
- When more than one Native Application is defined for automatic connection or disconnection, the applications run in the alphabetical order of the names of the Native Applications.

Use Case 1 - Automatically Map and Unmap a Network Drive

One example of how automatically running a command can be useful is to mount or unmount a network drive. Giving users access to network drives is a convenient way of providing access to internal resources. A drive can be mapped by configuring an application that invokes the Windows "`net use`" command.

It is possible to extend this ability by defining a dynamic add-on Downloaded-from-Gateway application that runs a script (batch file) containing a sequence of commands to execute on the endpoint machine. This script can be launched manually when the user clicks a link, or it can launch automatically after connecting to or disconnecting from SSL Network Extender.

Note - The "`net use`" command is available only for the SNX Network Mode.

Part 1 - Configure a Native Application to map (mount) the drive

1. Create a new Native Application or edit an existing Native Application to map (mount) the drive.
2. On the **Endpoint Applications** page, select **Add a link to the applicable in the Mobile Access portal**.
3. Select **Advanced**.
4. Click **Edit**.

   The **Endpoint Applications - Advanced** window opens.
5. Click **Add**.

   The **Edit Endpoint Application** window opens.
6. Select **Already installed**.
7. In the **Path and executable name** field, enter:

```
net.exe
```

8. In the **Parameters** field, enter:

```
use Drive_Letter: \\Server_Name\Share_Name
```

9. At the bottom of this page, click **Advanced**.
10. Select **When SSL Network Extender is launched**.
11. Click **OK** to close the **Advanced** window.
12. Click **OK** to close the **Edit Endpoint Application** window.
13. Click **OK** to close the **Endpoint Applications - Advanced** window.
14. Click **OK** to close the new Native Application object.

Part 2 - Configure a Native Application to unmap (unmount) the drive

1. Create a new Native Application or edit an existing Native Application to unmap (unmount) the drive.
2. On the **Endpoint Applications** page, select **Add a link to the applicable in the Mobile Access portal**.
3. Select **Advanced**.
4. Click **Edit**.

   The **Endpoint Applications - Advanced** window opens.
5. Click **Add**.

   The **Edit Endpoint Application** window opens.
6. Select **Already installed**.
7. In the **Path and executable name** field, enter:

```
net.exe
```

8. In the **Parameters** field, enter:

```
use /DELETE Drive_Letter:
```

9. At the bottom of this page, click **Advanced**.
10. Select **When SSL Network Extender is disconnected**.
11. Click **OK** to close the **Advanced** window.
12. Click **OK** to close the **Edit Endpoint Application** window.

13. Click **OK** to close the **Endpoint Applications - Advanced** window.
14. Click **OK** to close the new Native Application object.

Use Case 2 - Automatically Run a Script (Batch File)

It is possible to define a new Downloaded-from-Gateway Endpoint Application (embedded application) that runs a script (batch file) automatically after connecting to or disconnecting from SSL Network Extender.

Procedure

1. Create a batch (script) file containing a sequence of commands.
2. Define the batch file as a new Native Application for Client-Based Access.
3. Create a new Native Application or edit an existing Native Application.
4. On the **Endpoint Applications** page, select **Add a link to the applicable in the Mobile Access portal**.
5. Select **Advanced**.
6. Click **Edit**.

   The **Endpoint Applications - Advanced** window opens.
7. Click **Add**.

   The **Edit Endpoint Application** window opens.
8. At the bottom of this page, click **Advanced**.
9. Select the applicable option(s):
   - **When SSL Network Extender is launched**.
   - **When SSL Network Extender is disconnected**.

   For explanations, see *"Configuring Automatic Start of the Application" on page 37*.
10. Click **OK** to close the **Advanced** window.
11. Click **OK** to close the **Edit Endpoint Application** window.
12. Click **OK** to close the **Endpoint Applications - Advanced** window.
13. Click **OK** to close the new Native Application object.

Protection Levels for Native Applications

You can define a protection level for each native application. Configure this in the Properties window of each native application in **Additional Settings** > **Protection Level**.

The options are:

- **This application relies on the security requirements of the gateway**
  Rely on the Security Gateway security requirements. Users authorized to use the portal are also authorized to use this application. This is the default option.
- **This application has additional security requirements specific to the following protection level**
  Associate the Protection Level with the application. Users must be compliant with the security requirement for this application in addition to the requirements for the portal.

Defining Protection Levels

To access the Protection Level page from the Mobile Access tab

1. In SmartConsole, select **Security Policies > Shared Policies > Mobile Access** and click **Open Mobile Access Policy in SmartDashboard**.

   SmartDashboard opens and shows the **Mobile Access** tab.
2. From the navigation tree click **Additional Settings > Protection Levels** page from the navigation tree.
3. Click **New** to create a new Protection Level or double-click an existing Protection Level to modify it.

   The **Protection Levels** window opens, and shows the **General Properties** page.

To access the Protection Level page from a Mobile Access application

1. In SmartConsole, click **Objects > Object Explorer** (Ctrl+E).
2. Search for the Mobile Access application.
3. Double-click the application.
4. From the navigation tree, select **Additional Setting > Protection Level**.
5. To create a new Protection Level, select **Manage > New**.
6. To edit the settings of a Protection Level, select the Protection Level from the drop down list and then select **Manage > Details**.

   The **Protection Levels** window opens, and shows the **General Properties** page.

To configure the settings for a Protection Level

1. From the **General Properties** page in the **Protection Level** window, enter the **Name** for the Protection Level (for a new Protection Level only).
2. In the navigation tree, click **Authentication** and select one or more authentication methods from the available choices. Users accessing an application with this Protection Level must use one of the selected authentication schemes.
3. If necessary, select **User must successfully authenticate via SMS**.
4. In the navigation tree, click **Endpoint Security** and select one or both of these options:
   - **Applications using this Protection Level can only be accessed if the endpoint machine complies with the following Endpoint compliance policy**. Also, select a policy. This option gives access to the associated application only if the scanned client computer complies with the selected policy.
   - **Applications using this Protection Level can only be accesses from within Secure Workspace**. This option requires Secure Workspace to be running on the client computer.
5. Click **OK** to close the **Protection Level** window.
6. Install the Access Control Policy.

Adding Downloaded-from-Gateway Endpoint Applications

You can add Downloaded-from-Gateway applications to customize Mobile Access, in addition to the built-in applications.

This section explains how, and gives detailed examples.

Downloaded-from-Gateway Application Requirements

Downloaded-from-gateway applications are either Java-based applications or single executable applications (including batch files):

Application	Requirements
Java-based	■ Application must be packaged into a JAR file. ■ The JVM of a version required by the application must be installed on the endpoint machine. ■ The application must have a `Main` class.
Single executable	■ Must not require installation. ■ Must be platform-specific for Windows OS (EXE, BAT, CMD), Linux OS, or macOS.

Adding a New Application

To add a new downloaded-from-gateway endpoint application:

Part 1 - Prepare the application files

1. Compress your downloaded-from-gateway application file (JAR, EXE, and so on) into a CAB archive with the same name as the original file, but with a `.cab` file extension.

   To compress a file into a CAB archive , you can use the Microsoft Cabinet Tool `cabarc.exe` (you can download it from the Microsoft Web site).

2. Upload both your application file and the CAB archive to the Security Gateway to this directory:

   ```
   $CVPNDIR/htdocs/SNX/CSHELL/
   ```

3. Connect to the command line on the Security Gateway.

4. Log in to the Expert mode.

5. Assign the required permissions to the two files - your application file and the CAB archive:

   ```
   chmod -v 644 $CVPNDIR/htdocs/SNX/CSHELL/<Name-of-File>
   ```

Part 2 - Add and configure the container for the Endpoint Application in the management database

1. Close all SmartConsole clients connected to the Management Server.

   To see the current sessions in SmartConsole, go to **Manage & Settings** view > **Sessions** page.

2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. Go to **Table** > **Other** > **embedded_applications**.
4. In the top right panel, right-click an empty space and click **New**.
5. In the **Object** field, enter a name for the new Endpoint Application (spaces are not allowed) and click **OK**.
6. In the top right panel, select the new application object.
7. In the bottom panel, configure the application properties:

   Double-click a field > configure or select the required value > click OK.

Field Name	Description
`display_name`	The application name, which will appear in the Native Application object properties.
`embedded_application_type`	The type of downloaded-from-gateway application. Choose one of the options in the **Valid Values** list: ▪ `java_applet` ▪ `linux_executable` ▪ `mac_executable` ▪ `windows_executable`)
`file_name`	The name of the application file (JAR, EXE, BIN) you placed in `$CPVNDIR/htdocs/SNX/CSHELL/` (not the CAB archive).
`post_custom_params`	Parameters concatenated after the value of the "`server_name_required_params`" field. Can be left blank.

Field Name	Description
`pre_custom_params`	Parameters concatenated before the value of the "`server_name_required_params`" field. Usually used when configuring a new downloaded-from-gateway Java application. In that case, specify the main class name of the Java application.
`server_name_required_params`	Specifies if the new downloaded-from-gateway application requires the server address to be configured in SmartConsole in the Native Application object properties (in the Native Application object, click the **Endpoint Application** page > select **Add a link to the application in the Mobile Access portal** > select **Advanced** > click **Edit** > click **Add** > select **Downloaded from Mobile Access** > refer to the **Parameters** field). Values: ■ `true` - The application requires the server address to be configured ■ `false` - The application does not require the server address to be configured (this is the default)
`type`	Leave the default value "`embedded_application`".

8. Save the changes (**File** menu > **Save All**).
9. Close the Database Tool (GuiDBEdit Tool).

Part 3 - Configure the Native Application

1. Connect with SmartConsole to the Management Server.
2. Publish the SmartConsole session to make the new downloaded-from-gateway application available in SmartConsole.
3. Configure the applicable Native Application:
   a. At the top, click the **Objects** menu > **More object types** > **Custom Application/Site** > **Mobile Application** > **New Native Application**.

      Alternatively, in the top right corner, in the **Objects** panel, click **New** > **More** > **Custom Application/Site** > **Mobile Application** > **Native Application**.

b. On the **General Properties** page:

Instructions

i. In the **Name** field, enter the name for this object.

ii. **Optional:** In the **Comment** field, enter the description of this object.

iii. In the **Advanced** section, click **Connection direction** > select the applicable option > click **OK**.

c. On the **Authorized Locations** page:

Instructions

Select and configure the applicable option to specify where the Native Application is hosted and ensure users can only access the specified locations using the specified services.

- **Simple** - To configure one pair of a host and services.
- **Advanced** - To configure several pairs of hosts and services.

d. On the **Endpoint Applications** page:

Instructions

i. Select **Add a link to the application in the Mobile Access portal**.

ii. Select and configure the applicable option.

- **Simple** - To configure an application that is installed on the endpoint computer.
- **Advanced** - To configure advanced application settings.

i. Click **Edit**.

ii. In the **Endpoint Applications - Advanced** window, click **Add**.

iii. Select **Add a link to the application in the Mobile Access portal**.

iv. In the **Link text** field, enter the text for the link, on which the end users click to download the CAB archive.

v. **Optional:** In the **Tooltip** field, enter the applicable description for the application.

vi. Select **Downloaded from Mobile Access**.

vii. In the **Name** field, select the Endpoint Application that you configured in the Database Tool (GuiDBEdit Tool).

viii. In the **Parameters** field, enter the server address, to which the Endpoint Application connects.

ix. **Optional:** Click **Advanced** > configure the applicable settings > click **OK**.

x. Click **OK** to close the **Edit Endpoint Application** window.

xi. Click **OK** to close the **Endpoint Applications - Advanced** window.

e. In the **Additional Settings** section, on the **Protection Level** page:

Instructions

Select and configure the applicable option:

- **This application relies on the security requirements of the gateway**

  Configures the Native Application to rely on the gateway security requirement.

  Users who have been authorized to the portal, are authorized to this application.

  This is the default option.

- **This application has additional security requirements specific to the following protection level**

  Configures the Native Application to associate the Protection Level with the application.

  Users are required to be compliant with the security requirement for this application in addition to the requirements of the portal.

f. Click **OK** to close the **Native Application** window.

Part 4 - Assign the Native Applications to the user group

In the Mobile Access Policy, configure the applicable rules - select the Native Applications for the applicable user groups.

Part 5 - Install the policy

Install the Access Control policy.

Use Case: Adding a New SSH Application

This example adds two applications to Mobile Access as new downloaded-from-Mobile Access applications.

Description

1. SSH2 Java application:
   - JAR file name: `ssh2.jar`
   - Main class name: `ssh2.Main`
   - The application gets the SSH server address as a parameter.
   - Name in SmartConsole: `Jssh2_Client`

2. SSH2 Windows OS executable:
   - Executable file name: `WinSsh2.exe`
   - The application gets the SSH server address as a parameter.
   - Name in SmartConsole: `Wssh2_Client`

Part 1 - Prepare the application files

1. Compress the `ssh2.jar` application file into the `ssh2.cab` archive:

   ```
   cabarc.exe -m LZX:20 -s 6144 N ssh2.cab ssh2.jar
   ```

2. Compress the `WinSsh2.exe` application file into the `WinSsh2.cab` archive:

   ```
   cabarc.exe -m LZX:20 -s 6144 N WinSsh2.cab WinSsh2.exe
   ```

3. Upload all four files to the Security Gateway to the `$CVPNDIR/htdocs/SNX/CSHELL/` directory:
   - `ssh2.jar`
   - `ssh2.cab`
   - `WinSsh2.exe`
   - `WinSsh2.cab`
4. Connect to the command line on the Security Gateway.
5. Log in to the Expert mode.
6. Assign the required permissions to all four files:

   ```
   chmod -v 644 $CVPNDIR/htdocs/SNX/CSHELL/ssh2.jar
   chmod -v 644 $CVPNDIR/htdocs/SNX/CSHELL/ssh2.cab
   chmod -v 644 $CVPNDIR/htdocs/SNX/CSHELL/WinSsh2.exe
   chmod -v 644 $CVPNDIR/htdocs/SNX/CSHELL/WinSsh2.cab
   ```

Part 2 - Add and configure the Endpoint Application containers in the management database

1. Close all SmartConsole clients connected to the Management Server.

   To see the current sessions in SmartConsole, go to **Manage & Settings** view > **Sessions** page.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. Go to **Table** > **Other** > **embedded_applications**.
4. Configure the SSH2 Java-based Endpoint Application:

a. In the top right panel, right-click an empty space and click **New**.

b. In the **Object** field, enter this string and click **OK**:

```
Jssh2_Client
```

c. In the top right panel, select the new application object.

d. In the bottom panel, configure the application properties:

Field Name	Value
display_name	Jssh2_Client
embedded_application_type	java_applet
file_name	ssh2.jar
post_custom_params	Leave empty
pre_custom_params	ssh2.Main
server_name_required_params	true
type	embedded_application

5. Configure the SSH2 Windows OS Endpoint Application:

a. In the top right panel, right-click an empty space and click **New**.

b. In the **Object** field, enter this string and click **OK**:

```
Wssh2_Client
```

c. In the top right panel, select the new application object.

d. In the bottom panel, configure the application properties:

Field Name	Value
`display_name`	`Wssh2_Client`
`embedded_application_type`	`windows_executable`
`file_name`	`WinSsh2.exe`
`post_custom_params`	Leave empty
`pre_custom_params`	Leave empty
`server_name_required_params`	`true`
`type`	`embedded_application`

6. Save the changes (**File** menu > **Save All**).
7. Close the Database Tool (GuiDBEdit Tool).

Part 3 - Configure the Native Application for the SSH2 Java-based application

1. Connect with SmartConsole to the Management Server.
2. Publish the SmartConsole session to make the new downloaded-from-gateway application available in SmartConsole.
3. Configure the required Native Application:
   a. At the top, click the **Objects** menu > **More object types** > **Custom Application/Site** > **Mobile Application** > **New Native Application**.
   b. On the **General Properties** page:

      Instructions

      i. In the **Name** field, enter:

      `SSH2-Java-based`

      ii. **Optional:** In the **Comment** field, enter:

      `This is an SSH2 Java-based application`

      iii. In the **Advanced** section, click **Connection direction** > select **Client to server** > click **OK**.

c. On the **Authorized Locations** page:

Instructions

i. Select **Simple**.

ii. In the **Host/Address Range/Group** field, select the object that represents the SSH server.

If such object does not exist yet, you can create it from this page.

iii. In the **Service** field, select the object `ssh_version_2`.

d. On the **Endpoint Applications** page:

Instructions

i. Select **Add a link to the application in the Mobile Access portal**.

ii. Select **Advanced**.

iii. Click **Edit**.

iv. In the **Endpoint Applications - Advanced** window, click **Add**.

v. Select **Add a link to the application in the Mobile Access portal**.

vi. In the **Link text** field, enter:

```
SSH2 Java-based application
```

vii. **Optional:** In the **Tooltip** field, enter:

```
This is an SSH2 Java-based application
```

viii. Select **Downloaded from Mobile Access**.

ix. In the **Name** field, select this Endpoint Application:

```
Jssh2_Client
```

x. In the **Parameters** field, enter the SSH server IP address.

xi. Click **OK** to close the **Edit Endpoint Application** window.

xii. Click **OK** to close the **Endpoint Applications - Advanced** window.

e. Click **OK** to close the **Native Application** window.

Part 3 - Configure the Native Application for the SSH2 Windows OS application

1. Configure the required Native Application:

a. At the top, click the **Objects** menu > **More object types** > **Custom Application/Site** > **Mobile Application** > **New Native Application**.

b. On the **General Properties** page:

Instructions

i. In the **Name** field, enter:

```
SSH2-Windows-OS
```

ii. **Optional:** In the **Comment** field, enter:

```
This is an SSH2 application for Window OS
```

iii. In the **Advanced** section, click **Connection direction** > select **Client to server** > click **OK**.

c. On the **Authorized Locations** page:

Instructions

i. Select **Simple**.

ii. In the **Host/Address Range/Group** field, select the object that represents the SSH server.

If such object does not exist yet, you can create it from this page.

iii. In the **Service** field, select the object `ssh_version_2`.

d. On the **Endpoint Applications** page:

Instructions

i. Select **Add a link to the application in the Mobile Access portal**.

ii. Select **Advanced**.

iii. Click **Edit**.

iv. In the **Endpoint Applications - Advanced** window, click **Add**.

v. Select **Add a lin to the application in the Mobile Access portal**.

vi. In the **Link text** field, enter:

```
SSH2 application for Windows OS
```

vii. **Optional:** In the **Tooltip** field, enter:

```
This is an SSH2 application for Window OS
```

viii. Select **Downloaded from Mobile Access**.

ix. In the **Name** field, select this Endpoint Application:

```
Wssh2_Client
```

x. In the **Parameters** field, enter the SSH server IP address.

xi. Click **OK** to close the **Edit Endpoint Application** window.

xii. Click **OK** to close the **Endpoint Applications - Advanced** window.

e. Click **OK** to close the **Native Application** window.

Part 4 - Assign the Native Application to the user group

In the Mobile Access Policy, configure the applicable rules - select the Native Applications "`SSH2-Java-based`" and "`SSH2-Windows-OS`" for the applicable user groups.

Part 5 - Install the policy

Install the Access Control policy.

Use Case: Adding a New Microsoft Remote Desktop Profile

This example demonstrates how to configure Mobile Access to work with Microsoft Remote Desktop, with a predefined profile.

It also shows how to configure the profile per user group.

Part 1 - Create the Remote Desktop Profile

Create the RDP profile file (with an *.rdp* extension) using Microsoft Remote Desktop Connection: `%SystemRoot%\system32\mstsc.exe`

When creating the profile, you can define the address, the settings, applications that should run at log in, and more.

In this example, the profile file has the name of the relevant user group.

For a user group called `MyGroup1`, save a profile file with this name: `RDP_Profile_for_MyGroup1.rdp`

Part 2 - Prepare the application file

1. Compress the RDP profile `RDP_Profile_for_MyGroup1.rdp` file into the `RDP_Profile_for_MyGroup1.cab` archive:

   ```
   cabarc.exe -m LZX:20 -s 6144 N RDP_Profile_for_MyGroup1.cab
   RDP_Profile_for_MyGroup1.rdp
   ```

2. Upload the two files to the Security Gateway to the `$CVPNDIR/htdocs/SNX/CSHELL/` directory:
   - `RDP_Profile_for_MyGroup1.rdp`
   - `RDP_Profile_for_MyGroup1.cab`
3. Connect to the command line on the Security Gateway.
4. Log in to the Expert mode.
5. Assign the required permissions to all four files:

   ```
   chmod -v 644 $CVPNDIR/htdocs/SNX/CSHELL/RDP_Profile_for_
   MyGroup1.rdp
   ```

   ```
   chmod -v 644 $CVPNDIR/htdocs/SNX/CSHELL/RDP_Profile_for_
   MyGroup1.cab
   ```

Part 3 - Add and configure the Endpoint Application container in the management database

1. Close all SmartConsole clients connected to the Management Server.

   To see the current sessions in SmartConsole, go to **Manage & Settings** view > **Sessions** page.

2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. Go to **Table** > **Other** > **embedded_applications**.
4. Configure the required Native Application:

a. In the top right panel, right-click an empty space and click **New**.

b. In the **Object** field, enter this string and click **OK**:

```
RDP_Profile_for_MyGroup1
```

c. In the top right panel, select the new application object.

d. In the bottom panel, configure the application properties:

Field Name	Value
display_name	RDP_Profile_for_MyGroup1
embedded_application_type	windows_executable
file_name	RDP_Profile_for_MyGroup1.rdp
post_custom_params	Leave empty
pre_custom_params	Leave empty
server_name_required_params	false
type	embedded_application

5. Save the changes (**File** menu > **Save All**).
6. Close the Database Tool (GuiDBEdit Tool).

Part 4 - Configure the Native Application for the Windows Remote Desktop application

1. Connect with SmartConsole to the Management Server.
2. Publish the SmartConsole session to make the new downloaded-from-gateway application available in SmartConsole.
3. Configure the required Native Application:
   a. At the top, click the **Objects** menu > **More object types** > **Custom Application/Site** > **Mobile Application** > **New Native Application**.

b. On the **General Properties** page:

Instructions

i. In the **Name** field, enter:

```
Windows-Remote-Desktop-for-MyGroup1
```

ii. **Optional:** In the **Comment** field, enter:

```
This is a Windows Remote Desktop application for
'MyGroup1'
```

iii. In the **Advanced** section, click **Connection direction** > select **Client to server** > click **OK**.

c. On the **Authorized Locations** page:

Instructions

i. Select **Simple**.

ii. In the **Host/Address Range/Group** field, select the object that represents the Windows server.

If such object does not exist yet, you can create it from this page.

iii. In the **Service** field, select the object `RDP`.

d. On the **Endpoint Applications** page:

Instructions if user needs to start the Remote Desktop application manually

i. Select **Add a link to the application in the Mobile Access portal**.

ii. Select **Simple**.

iii. In the **Link text** field, enter:

```
Windows Remote Desktop application
```

iv. **Optional:** In the **Tooltip** field, enter:

```
This is a Windows Remote Desktop application for
'MyGroup1'
```

v. In the **Path and executable name** field, enter:

```
%SystemRoot%\system32\mstsc.exe
```

vi. In the **Parameters** field, enter:

```
%temp%\RDP_Profile_for_MyGroup1.rdp
```

Instructions if it is necessary to start the Remote Desktop application automatically

It is necessary to configure two Endpoint Applications - one to download the RDP profile, and another to trigger this download as soon as SSL Network Extender is launched.

i. Select **Add a link to the application in the Mobile Access portal**.

ii. Select **Advanced**.

iii. Click **Edit**.

iv. In the **Endpoint Applications - Advanced** window, click **Add**.

v. Select **Add a link to the application in the Mobile Access portal**.

vi. In the **Link text** field, enter:

```
Windows Remote Desktop application
```

vii. **Optional:** In the **Tooltip** field, enter:

```
This is a Windows Remote Desktop application for
'MyGroup1'
```

viii. Select **Already installed**.

ix. In the **Path and executable name** field, enter:

```
%SystemRoot%\system32\mstsc.exe
```

x. In the **Parameters** field, enter:

```
%temp%\RDP_Profile_for_MyGroup1.rdp
```

xi. Click **OK** to close the **Edit Endpoint Application** window.

xii. In the **Endpoint Applications - Advanced** window, click **Add**.

xiii. Clear **Add a link to the application in the Mobile Access portal**.

xiv. Select **Downloaded from Mobile Access**.

xv. In the **Name** field, select this Endpoint Application:

```
RDP_Profile_for_MyGroup1
```

xvi. In the **Parameters** field, do not enter anything.

xvii. Click **Advanced** > select **When SSL Network Extender is launched** > click **OK**.

xviii. Click **OK** to close the **Edit Endpoint Application** window.

xix. Click **OK** to close the **Endpoint Applications - Advanced** window.

e. Click **OK** to close the **Native Application** window.

Part 5 - Assign the Native Application to the user group

In the Mobile Access Policy, configure the applicable rules - select the Native Application "`Windows-Remote-Desktop-for-MyGroup1`" for the applicable user groups.

Part 6 - Install the policy

Install the Access Control policy.

Configuring Downloaded-from-Gateway Endpoint Applications

In the **Endpoint Applications** page of the Native Application object:

1. Select **Add link in the Mobile Access Portal**.
2. Select **Advanced > Edit**.

   The **Endpoint Applications - Advanced** window opens.
3. Click **Add**.

   The **Edit Endpoint Application** window opens.
4. Select **Downloaded-from-Gateway**.
5. From the **Name** drop-down list, select the applicable downloaded-from-gateway application.
6. Specify the **Parameters** for the downloaded-from-Security Gateway application. The parameters field is used to pass additional information to the downloaded-from-gateway applications on the endpoint machine, and to configure the way they are launched.

   The `$$user` variable can be used here to dynamically change according to the login name of the currently logged in user.

   See the configuration sections below for details of the required parameters:

   Note - In the configuration sections for certified and add-on applications, below:
   - `parameter` is a mandatory parameter,
   - `[parameter]` is an optional parameter,
   - `|` indicates a required choice of one from many.

- **Configuring the Telnet Client (Certified Application)**

Supported Platforms	All
Parameters field	Server name or IP address. Default port is 23.
Parameters usage	`server [port]`
Description	Telnet terminal. Provides user oriented command line login sessions between hosts on the Internet.
Home page	http://javassh.org

- **Configuring the SSH Client (Certified Application)**

Supported Platforms	All
Parameters field	Server name or IP address.
Parameters usage	`server`
Description	Secure Shell (SSH) is designed for logging into and executing commands on a networked computer. It provides secure encrypted communications between two hosts over an insecure network. An SSH server, by default, listens on the standard TCP port 22.
Home page	http://javassh.org

- **Configuring the TN3270 Client (Certified Application)**

Supported Platforms	All. Requires Java 1.3.1 or higher.
Parameters field	Ignored
Description	IBM 3270 terminal emulator tailored to writing screen-scraping applications. TN3270 is the remote-login protocol used by software that emulates the IBM 3270 model of mainframe computer terminal.
Home page	http://jagacy.com

- **Configuring the TN5250 Client (Certified Application)**

Supported Platforms	All endpoint machines must have Java 1.4 or higher.
Parameters field	Optional. Can use the Configure button on the application instead. For the full list of options that can be used in the parameters field, see the Quick Start Guide http://tn5250j.sourceforge.net/quick.html.
Parameters usage	`[server [options]]`
Description	IBM 5250 terminal emulator that interprets and displays 5250 data streams. You will be presented with a Connections screen for defining sessions. Select the configure button to define sessions when the session selection window opens. On first invocation of the emulator there are some console warning messages. These inform you that defaults files are being set up for the first run.
Home page	http://tn5250j.sourceforge.net/index.html
Quick Start Guide	http://tn5250j.sourceforge.net/quick.html

- **Configuring the Remote Desktop Client (Add-On Application)**

Supported Platforms	All platforms. Endpoint machines must have Java 1.4 or higher.
Parameters field	Must contain the server name or its IP address.
Parameters usage	`[options] server[:port]` For example: `-g 800x600 -l WARN RDP_Server` Options: • `-b` - Bandwidth saving (good for 56k modem, but higher latency). This option clears the TCP 'no delay' flag. • `-d` - Windows domain you are connecting to. • `-f` - Show the window full-screen (requires Java 1.4 for proper operation). • `-g` - The size of the desktop in pixels (width x height). • `-m` - Keyboard layout on terminal server for languages (for example, en-us). • `-l {DEBUG, INFO, WARN, ERROR, FATAL}` - Amount of debug output (otherwise known as the logging level). • `-lc` - Path to a log4j configuration file. • `-n` - Override the name of the endpoint machine. • `-u` - Name of the user to connect as. • `-p` - Password for the above user. • `-s` - Shell to launch when the session is started. • `-t` - Port to connect to (useful if you are using an SSH tunnel, for example). • `-T` - Override the window title.
Description	Downloaded-from-Mobile Access Client for Windows NT Terminal Server and Windows 2000/2003 Terminal Services. Communicates using Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required. Runs on Java 1.1 up (optimized for 1.4), and works on Linux, Windows and Mac.
Home page	http://properjavardp.sourceforge.net

- **Configuring the PuTTY Client (Add-On Application)**

Supported Platforms	Windows only
Parameters field	Optional. Leaving the Parameters field empty leads PuTTY Client to open in full graphical mode.
Parameters usage	`[[-ssh | -telnet | -rlogin | -raw] [user@]server [port]]`
Description	An implementation of Telnet and SSH for Win32 platforms, including an Xterm terminal emulator.
Home page	http://www.eos.ncsu.edu/remoteaccess/putty.html

- **Configuring the Jabber Client (Add-On Application)**

Supported Platforms	All platforms. Endpoint machines must have Java 1.4 or higher.
Parameters field	Ignored
Description	Downloaded-from-Gateway Jabber Client is an instant messenger based on the Jabber protocol Runs on every computer with at least Java 1.4.
Home page	http://jeti.jabberstudio.org

- **Configuring the FTP Client (Add-On Application)**

Supported Platforms	All endpoint machines must have Java 1.4 or higher.
Parameters field	Ignored
Description	Graphical Java network and file transfer client. Supports FTP using its own FTP API and various other protocols like SMB, SFTP, NFS, HTTP, and file I/O using third party APIs, includes many advanced features such as recursive directory up/download, browsing FTP servers while transferring files, FTP resuming and queuing, browsing the LAN for Windows shares, and more.
Home page	http://j-ftp.sourceforge.net

7. Configure Native Applications for Client-Based Access.

SSL Network Extender (SNX) for Remote Access VPN

Basic Configuration of SSL Network Extender for Remote Access VPN

Configuring the Security Gateway for SSL Network Extender

Step 1 - Configure the applicable Remote Access VPN Community

1. In SmartConsole, in the top right panel **Objects**, click **VPN Communities**.
2. Right-click the **RemoteAccess** object and click **New**.
3. Configure the required settings:
    a. Object name.
    b. Participating Security Gateways.
    c. Participant User Groups.
4. Click **OK**.

Step 2 - Configure the IPsec VPN settings in the Security Gateway / ClusterXL object

See the *Site to Site VPN Administration Guide* for your version.

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway.
3. From the navigation tree, click **General Properties**.
4. Select the **IPsec VPN** Software Blade.
5. From the navigation tree, click **IPsec VPN**.
6. To add the Security Gateway to a Remote Access community:
    a. Click **Add**.
    b. Select the community.
    c. Click **OK**.
7. From the navigation tree, expand **Network Management** and click **VPN Domain**.

8. Configure the applicable VPN Domain.
9. Configure the settings for **Visitor Mode** (see the *Remote Access VPN Administration Guide* for your version > "Configuring Remote Access Connectivity" chapter > "Configuring Windows Proxy Replacement" section > "Proxy Replacement for the Security Gateway" heading).
10. From the navigation tree, expand **VPN Clients** and click **Office Mode**.
11. Configure the settings for **Office Mode** (see the *Remote Access VPN Administration Guide* for your version > "Office Mode" chapter > "IP Pool Configuration" heading).

    Note - Office Mode support is mandatory on the Security Gateway / Cluster.

12. Click **OK**.

Step 3 - Configure the SSL Network Extender settings in the Security Gateway / ClusterXL object

Important - If the Mobile AccessSoftware Blade is enabled on a Security Gateway, then SSL Network Extender works through Mobile Access and not IPsec VPN.
In this case, you must configure the SSL Network Extender settings in the Mobile AccessSoftware Blade.
If you already had SSL Network Extender settings configured in the IPsec VPNSoftware Blade and then you enabled the Mobile AccessSoftware Blade, then you must configure the SSL Network Extender settings for the Mobile AccessSoftware Blade.

See the *Mobile Access Administration Guide* for your version.

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. From the navigation tree, click **General Properties**.
4. Select the **Mobile Access** Software Blade.
5. In the **Mobile Access Configuration** wizard:
   a. On the **Mobile Access** page, you must select **Web** (you can select other applicable options).

      Click **Next**.

   b. On the **Web Portal** page, configure the applicable Main URL and Portal Certificate.

      Click **Next**.

c. On the **Applications** page, configure the applicable options.

   Click **Next**.

d. On the **Active Directory Integration** page, configure the applicable settings.

   Click **Next**.

e. On the **Authorized Users** page, configure the applicable settings.

   Click **Next**.

f. On the **Applications** page, configure the applicable settings.

   Click **Next**.

g. Click **Finish**.

6. From the navigation tree, click **Mobile Access**.

   In the **Allowed Clients** section, make sure **Web** is selected.

7. From the navigation tree, click **VPN Clients**:

   a. Make sure **Other** is selected and **SSL Network Extender (SNX)** is selected.

   b. From **The gateway authenticates with this certificate**, select the certificate that is used to authenticate to all SSL clients.

8. Click **OK**.

Step 4 - Configure the SSL Network Extender settings in the Global Properties

1. From the top left Menu, click **Global properties**.
2. From the left, expand **Remote Access** and click **SSL Network Extender**.
3. In the **User Authentication** section, from the **User authentication method**, select the applicable method:

   - **Certificate** - The system authenticates the user only with a certificate.
   - **Certificate with enrollment** - The system authenticates the user only with a certificate. Enrollment is allowed.

     If the users do not have a certificate, they can enroll using a registration key that they previously received from the administrator.

     For more information about creating a user certificate for enrollment, see *"Management of Internal Certificate Authority (ICA) Certificates" on page 81*.

- **Legacy** - The system authenticates the user with the **Username** and **Password**. This is the default setting.
- **Mixed** - The system tries to authenticate the user with the certificate. If the user does not have a valid certificate, the system tries to authenticate the user with the **Username** and **Password**.

4. Click **OK**.

Step 5 - Install the Security Policy

1. From the top, click **Install Policy**.
2. Select the applicable Security Policy.
3. Select **Access Control**.
4. Select the Security Gateway / Cluster object.
5. Click **Install**.

Downloading and Connecting the SNX Client

Downloading and Connecting the SNX Client for Windows

1. Using Internet Explorer, browse to the SSL Network Extender portal of the Security Gateway at:

   ```
   https://<IP Address or HostName of Security Gateway>
   ```

   This Security Alert message may appear:

   ```
   The site's security certificate has been issued by an
   authority that you have not designated as a trusted CA.
   Before you connect to this server, you must trust the CA
   that signed the server certificate. (The system
   administrator can define which CAs may be trusted by the
   user.) You can view in the certificate in order to decide if
   you wish to proceed.
   ```

   Note - The administrator can direct the user to the URL below to install this CA certificate, thereby establishing trust, and to avoid this message in the future:

   ```
   http://<IP Address of Management Server>:18264
   ```

2. Click **Yes**.

   If Endpoint Security on Demand is enabled, the **ESOD web page** opens.

If this is the first time that the user is scanned with ESOD, the user should install the ESOD ActiveX object.

If this is the first time that ESOD is used, the **Server Confirmation** window appears. The user must confirm that the listed ESOD server is identical to the organization's site for remote access.

3. Click one of these:
   - **No** - An error message appears and the user is denied access.
   - **Yes** - The ESOD client continues the software scan. Moreover, if the **Save this confirmation for future use** is selected, the **Server Confirmation** window does not appear the next time the user attempts to log in.

   After the user confirms the ESOD server, an automatic software scan takes place on the client's machine.

   When the scan completes, the scan results and directions on how to proceed appear.

ESOD not only prevents users with potentially harmful software from accessing your network, but also requires that they conform to the corporate Anti-Virus and firewall policies, as well. A user is defined as having successfully passed the ESOD scan only if he/she successfully undergoes scans for *Malware*, *Anti-Virus*, and *Firewall*. Each malware appear as a link, which, if selected, redirects you to a data sheet describing the detected malware. The data sheet includes the name and a short description of the detected malware, what it does, and the recommended removal method(s).

The options available to the user are configured by the administrator on the ESOD server:

Scan Option	Description
Scan Again	Allows a user to rescan for malware. This option is used in order to get refreshed scan results, after manually removing an unapplicable software item.
Cancel	Prevents the user from proceeding with the portal login, and closes the current browser window.
Continue	Causes the ESOD for Mobile Access client to disregard the scan results and proceed with the log on process.

To continue with the download:

1. From the **Scan Results**, select a different language from the list.

   If you change languages, while connected to the SSL Network Extender portal, the portal informs you that if you continue the process it disconnects you, and you must connect again.

2. From the **Scan Results**, you can select a different skin from the **Skin** drop-down list . You can change skins, while connected to the SSL Network Extender portal.

3. Click **Continue**.

   - If the configured authentication scheme is **User Password Only**, an **SSL Network Extender Login** window appears.

     Enter the **User Name** and **Password** and click **OK**.

     Note - If user authentication has been configured to be performed via a 3rd party authentication mechanism, such as SecurID or LDAP, the Administrator may require the user to change his/her PIN, or Password. In such a case, an additional Change Credentials window appears, before the user is allowed to access the SSL Network Extender.

   - If the configured authentication scheme is **Certificate without Enrollment**, and the user already has a certificate. If the user does not already have a certificate, access is denied.

   - If the configured authentication scheme is **Certificate with Enrollment**, and the user does not already have a certificate, the **Enrollment** window appears.

4. Enter the **Registration Key** and select **PKCS#12 Password**.

5. Click **OK**.

   The PKCS#12 file is downloaded.

   At this point the user should open the file and utilize the Microsoft Certificate Import wizard as follows.

   Best Practice - We strongly recommend that the user set the property **Do not save encrypted pages to disk** on the **Advanced** tab of the **Internet Properties** of Internet Explorer. This prevents the certificate from being cached on disk.

Importing a Client Certificate with the Microsoft Certificate Import Wizard to Internet Explorer:

The web browser automatically uses the client certificate when SSL Network Extender connects to a Security Gateway.

To import a client certificate:

1. Open the downloaded PKCS#12 file.

   The **Certificate Import Wizard** opens.

2. Click **Next**.

   The **File to Import** window opens.

   The P12 file name appears.

3. Click **Next**.

   The **Password** window appears.

   We strongly recommend to enable **Strong Private Key Protection**.

   The user is then be prompted for consent/credentials, as configured, each time authentication is required.

   Otherwise, authentication is fully transparent for the user.

4. Enter your password, click **Next** twice.

   If the user enabled **Strong Private Key Protection**, the **Importing a New Private Exchange Key** window appears:

   - If you click **OK**, the Security Level is assigned the default value **Medium**, and the user is asked to consent each time the certificate is required for authentication.
   - If you click **Set Security Level**, the **Set Security Level** window appears. Select either **High** or **Medium**, and click **Next**.

5. Click **Finish**.

   The **Import Successful** window appears.

6. Click **OK**.

7. Close and reopen your browser.

   You can now use the certificate that has now been imported for logging in.

8. If you are connecting to the SSL Security Gateway for the first time, a VeriSign certificate message appears, requesting the user's consent to continue installation.

- If you connect using Java Applet, a Java security message appears. Click **Yes**.
- If the system administrator configured the upgrade option, the Upgrade Confirmation window appears:

  If you click **OK**, you must re-authenticate and a new SSL Network Extender version is installed.
- If you click **Cancel**, the client connects normally.

  (The **Upgrade Confirmation** window does not appear again for a week.)

  The **SSL Network Extender** window appears.

  A **Click here to upgrade** link appears in this window, enabling the user to upgrade even at this point.

  If you click the **Click here to upgrade** link, you must authenticate again before the upgrade can proceed.

9. At first connection, the user is notified that the client is associated with a specific Security Gateway. Click **Yes**.

   The server certificate of the Security Gateway is authenticated.

   If the system Administrator has sent the user a *fingerprint*, it is strongly recommended that the user verify that the root CA fingerprint is identical to the fingerprint, sent to the user.

   The system Administrator can view and send the fingerprint of all the trusted root CAs, in the **Certificate Authority Properties** window in SmartConsole.

10. If the user is using a proxy server that requires authentication, the **Proxy Authentication** pop-up appears.

    The user must enter his/her proxy username and password, and click **OK**.

11. If you connect on Windows OS, a **Windows Firewall** message may appears. Click **Unblock**.

    You may work with the client as long as the **SSL Network Extender Connection** window remains open, or minimized (to the system tray).

    Once the SSL Network Extender is initially installed, a new Windows service named **Check PointSSL Network Extender** and a new virtual network adapter are added.

Notes:

- The settings of the adapter and the service must not be changed. IP assignment, renewal and release are done automatically.
- The Check Point SSL Network Extender service depends on both the virtual network adapter and the DHCP client service.
  Therefore, the DHCP client service must not be disabled on the user's computer.

Both the virtual network adapter and the Check Point SSL Network Extender service are removed during the product uninstall.

There is no need to reboot the client machine after the installation, upgrade, or uninstall of the product.

12. When you finish working, click **Disconnect** to terminate the session, or when the window is minimized, right-click the icon and click **Disconnect**. The window closes.

To remove an imported certificate:

If you imported a certificate to the browser, it remains in storage until you manually remove it.

We strongly recommend that you remove the certificate from a browser that is not yours.

Follow the instructions from the vendor of your web browser.

Downloading and Connecting the SNX Client for Linux or macOS

SNX is available for Linux and macOS endpoint computers only as a CLI application. For more information, see *"Using SSL Network Extender on Linux / macOS Operating Systems" on page 83*.

Prerequisites

- The endpoint computer must meet necessary prerequisites. For more information, see *"SSL Network Extender (SNX) Versions and Requirements" on page 16*.
- The endpoint computer must be able to connect directly to the Security Gateway that has SNX enabled.
- The user of the endpoint computer must have "execute" permissions to download a Shell archive to the user's home directory.
- The user of the endpoint computer must have administrator permissions or the root password.

For a workaround to download and connect SNX without administrator permissions or the root password for the endpoint computer, see *"Installation for Users without Administrator Privileges" on page 85*.

To download and connect the SNX client for Linux or macOS:

1. On the endpoint computer, in a web browser, go to the IP address or the FQDN of the Security Gateway.

   The **SSL Network Extender** homepage opens.

2. From the right menu, expand **Download SSL Network Extender manual installation**.

3. Select the appropriate option:

   - **Download command line SNX for Linux.**
   - **Download command line SNX for Macintosh.**

   The endpoint computer downloads the Shell archive package from the Security Gateway and saves it in the user's home directory.

4. Make sure that the user has "execute" permissions to download the Shell archive package to the user's home directory. To add the "execute" permissions, run:

   ```
   chmod + x snx_install.sh
   ```

5. Run the installation script:

   ```
   snx_install.sh
   ```

   If the user does not have administrator permissions, the endpoint computer asks the user to enter a root password. In this case, enter the root password and then press the `Enter` key.

   To disconnect after installation, run:

   ```
   Server_1:/ snx -d
   ```

Customizing the SSL Network Extender Portal

You can modify the SSL Network Extender Portal by changing skins and languages.

Changing the SNX Portal Skin

Configuring the Skins Option

To configure the Skins Option:

The `skin` directory is located inside the `$FWDIR/conf/extender` directory on the Security Gateways.

There are two subdirectories:

- `chkp`: contains skins that Check Point provides by default. During upgrade, this subdirectory may be overwritten.
- `custom`: contains skins defined by the customer. If this subdirectory does not exist yet, create it. During upgrade, this subdirectory is not overwritten. New skins are added in this subdirectory.

Disabling a Skin

1. Enter the specific skin subdirectory, in the `custom` directory that is to be disabled, and create a file named `disable`. This file may be empty.
2. If the specific skin does not exist in the `custom` directory, create it and then create a file within it named `disable`.
3. Install Policy.

   The next time that the user connects to the SSL Network Extender portal, this skin is not available.

Example

```
cd $FWDIR/conf/extender/skin/custom

mkdir skin1

touch disable
```

Creating a Skin

1. Enter the `custom` subdirectory.
2. Create a directory with the applicable skin name.

Note - Make sure this name is not already used in `chkp`. If it is, the new skin definition overrides the existing skin definition (as long as the new skin definition exists). Once you have deleted the new skin definition, the `chkp` skin definition is used again.

Each skin folder must contain these CSS files:

- `help_data.css` - The main OLH page uses this stylesheet.
- `help.css` - The inner frame on the OLH page uses this stylesheet.
- `index.css` - The ESOD pages, and the main SSL Network Extender portal page use this stylesheet.
- `style.css` - All login pages use this stylesheet.
- `style_main.css` - The main SSL Network Extender Connection page, Proxy Authentication page, and Certificate Registration page use this stylesheet.

Best Practice - We recommend that you copy these files from another `chkp` skin, and then modify them as applicable.

3. In SmartConsole, install policy.

Example

Add your company logo to the main SSL Network Extender portal page.

1. `cd $FWDIR/conf/extender/skin/custom`
2. `mkdir <skin_name>`
3. `cd <skin_name>`
4. `cp -v../../chkp/skin2/* .`
5. Place logo image file in this directory.
6. Edit the `index.css` file.
7. Go to `company_logo` and replace the existing URL reference with a reference to the new logo image file.
8. Save the changes in the file..
9. In SmartConsole, install policy.

Note - No spaces are allowed in the `<skin_name>`.

Changing the SNX Portal Language

Configuring the Languages Option

To configure the Languages Option:

The `languages` directory is located inside the `$FWDIR/conf/extender` directory on the Security Gateways.

There may be two subdirectories:

- `chkp` - Contains languages that Check Point provides by default. During upgrade, this subdirectory may be overwritten.
- `custom` - Contains languages defined by the customer. If `custom` does not exist yet, create it. During upgrade, this subdirectory is not overwritten. New languages are added in this subdirectory.

Disabling a Language

1. Enter the specific language subdirectory, in the `custom` directory that is to be disabled (if it exists) and create a file named `disable`. This file may be empty.
2. If the specific language does not exist in the `custom` directory, create it and then create a file within it named `disable`.
3. In SmartConsole, install policy.

   The next time that the user connects to the SSL Network Extender portal, this language is not be available.

Adding a Language

1. Enter the `custom` subdirectory.
2. Create a folder with the applicable language name.

   Note - Make sure this name is not already used in `chkp`. If it is, the new language definition overrides the existing language definition (as long as the new language definition exists). Once you have deleted the new language definition, the `chkp` language definition is used again.
3. Copy the `messages.js` file of an existing `chkp` language to this directory.
4. Edit the `messages.js` file and translate the text bracketed by quotation marks.
5. Save the changes in the file.
6. In SmartConsole, install policy.

Example

1. `cd $FWDIR/conf/extender/language`
2. `mkdir custom`
3. `cd custom`
4. `mkdir <language_name>`
5. `cd <language_name>`
6. `cp -v ../../chkp/english/messages.js .`
7. Edit the `messages.js` file and translate the text bracketed by quotation marks.
8. Save the changes in the file.
9. In the `custom/english/messages.js` file, add a line as follows:

   ```
   <language_name>="translation of language_name";
   ```

   Note - No spaces are allowed in the `<language_name>`.

10. Install the Access Control policy.

Modifying a Language

1. Enter the `custom` subdirectory.
2. Create a folder with a language name that matches the `chkp` language folder to be modified.
3. Create an empty `messages.js` file, and insert only those messages that you want to modify, in this format:

   ```
   <variable_name>="<applicable_text>";
   ```

   Note - For reference, refer to the `messages.js` file, located in `chkp/<language>`.

SSL Network Extender User Experience

This section describes the user experience, including downloading and connecting the SSL Network Extender client, importing a client certificate, and uninstalling on disconnect.

Configuring Microsoft Internet Explorer

Check Point SSL Network Extender uses ActiveX controls and cookies to connect to applications via the Internet.

These enabling technologies require specific browser configuration to ensure that the applications are installed and work properly on your computer.

The Trusted Sites Configuration approach includes the SSL Network Extender Portal as one of your Trusted Sites.

This approach is highly recommended, as it does not lessen your security. Please follow the directions below to configure your browser.

Configuration of Trusted Sites

1. In Internet Explorer, select **Tools > Internet Options > Security**.
2. Select **Trusted sites**.
3. Click **Sites**.
4. Enter the URL of the SSL Network Extender Portal and click **Add**.
5. Click **OK** twice.

About ActiveX Controls

ActiveX controls are software modules, based on Microsoft's Component Object Model (COM) architecture. They add functionality to software applications by seamlessly incorporating pre-made modules with the basic software package.

On the Internet, ActiveX controls can be linked to Web pages and downloaded by an ActiveX-compliant browser. ActiveX controls turn Web pages into software pages that perform like any other program.

The SSL Network Extender can use ActiveX control in its applications. To use ActiveX you must download the specific ActiveX components required for each application. Once these components are loaded, you do not need to download them again unless upgrades or updates become available. If you do not want to use an ActiveX component you may work with a Java Applet.

Note - You must have Administrator rights to install or uninstall software on Windows operating systems.

Management of Internal Certificate Authority (ICA) Certificates

If the administrator configured **Certificate with enrollment** as the user authentication method (**Menu** > **Global properties** > **Remote Access** > **SSL Network Extender**), users can create a certificate for their use, by using a registration key, provided by the system administrator.

To create a user certificate for enrollment:

1. Follow the procedure in the *Quantum Security Management Administration Guide* for your version > Section "The Internal Certificate Authority (ICA) and the ICA Management Tool".

   Note - This version does not support enrollment to an External CA.

2. Browse to the ICA Management Tool site and select **Create Certificates**:

   ```
   https://<IP address of Management Server>:18265
   ```

3. Enter the user's name, and click **Initiate** to receive a Registration Key, and send it to the user.

   When the user attempts to connect to the SSL Network Extender, without having a certificate, the **Enrollment** window appears, and the user can create a certificate by entering the Registration Key, received from the system administrator.

   For a description of the user login experience, see *"Management of Internal Certificate Authority (ICA) Certificates" above*.

   Note - The system administrator can direct the user to the URL below to allow the user to receive a Registration Key and create a certificate, even if they do not wish to use the SSL Network Extender, at this time.

   ```
   http://<IP Address of Security Gateway>/registration.html
   ```

4. You can determine whether the SSL Network Extender is upgraded automatically, or not.

   Select the client upgrade mode from the drop-down list:

   - **Do not upgrade** - Users of older versions are not be prompted to upgrade.
   - **Ask user** - (Default) Ask user whether or not to upgrade, when the user connects.

- **Force upgrade** - Every user, whether users of older versions or new users download and install the newest SSL Network Extender version.

  Note - Use the **Force upgrade** option only when the system administrator is sure that all the users have administrator privileges. Otherwise, the user cannot connect with SSL Network Extender.

For a description of the user upgrade experience, see *"Management of Internal Certificate Authority (ICA) Certificates" on the previous page*.

5. Select the supported encryption method from the drop-down list:
   - **3DES only** - (Default) The SSL Network Extender client supports 3DES, only.
   - **3DES or RC4** - The SSL Network Extender client supports the RC4 encryption method, as well as 3DES.
6. You can determine whether to uninstall SSL Network Extender automatically when the user disconnects.

   Select the applicable option from the drop-down list:
   - **Keep installed** - (Default) Do not uninstall. If the user wishes to uninstall the SSL Network Extender, he/she can do so manually.
   - **Ask user whether to uninstall** - Ask user whether or not to uninstall, when the user disconnects.
   - **Force uninstall** - Always uninstall automatically, when the user disconnects.

   For a description of the user disconnect experience, see *"Management of Internal Certificate Authority (ICA) Certificates" on the previous page*.

   Note - The Uninstall-on-Disconnect feature does not ask the user whether or not to uninstall, and does not uninstall the SSL Network Extender, if a user has entered a suspend/hibernate state, while the user was connected.
7. You can determine how to activate Endpoint Security on Demand.

   When Endpoint Security on Demand (ESOD) is activated, users attempting to connect to the SSL Network Extender are required to successfully undergo an ESOD scan before being allowed to access the SSL Network Extender.

   Select the applicable option from the drop-down list:
   - **None**
   - **Endpoint Security on Demand**

Using SSL Network Extender on Linux / macOS Operating Systems

SSL Network Extender Command Parameters

Parameter	Description
`snx -f <configuration file>`	Run SSL Network Extender using parameters defined in a configuration file other than the default name or location.
`snx -d`	Disconnect from Mobile Access
`snx -s <server>`	Specify server IP or hostname
`snx -u <username>`	Specify a valid user
`snx -c <certificate file>`	Specify which certificate is used to authenticate.
`snx -l <CA directory>`	Define the directory where CA's certificates are stored.
`snx -p <port>`	Change the HTTPS port. (default port is TCP 443).
`snx -g`	Enable debugging. The `snx.elg` log file is created.
`snx -e <cipher>`	Force a specific encryption algorithm. Valid values - RC4 and 3DES.

Configuration File Attributes

It is possible to predefine SSL Network Extender attributes by using a configuration file (`.snxrc`) located in the users home directory.

When the SSL Network Extender command SSL Network Extender is executed, the attributed stored in the file are used by the SSL Network Extender command.

To run a file with a different name execute the command `snx -f <filename>`.

Note - You can configure proxy server only in the configuration file and not directly from the command line.

Attributes	Description
`server`	Change the HTTPS port. (default port is TCP 443).
`sslport`	Change the HTTPS port. (default port is TCP 443).
`username`	Specify a valid user
`certificate`	Specify which certificate is used to authenticate
`calist`	Define the directory where CA's certificates are stored.
`debug`	Enable debugging. The `snx.elg` log file is created. Valid values {`yes`, `no`}. To activate debugging when running java, create a `.snxrc` file that contains the line "`debug yes`" in the home directory.
`cipher`	Force a specific encryption algorithm. Valid values: `RC4` and `3DES`
`proxy_name`	Define a Proxy hostname
`proxy_port`	Define a proxy port
`proxy_user`	Define a proxy user
`proxy_pass`	Define a password for proxy authentication

Installation for Users without Administrator Privileges

The SSL Network Extender usually requires Administrator privileges to install the ActiveX component. To allow users that do not have Administrator privileges to use the SSL Network Extender, the Administrator can use his/her remote corporate installation tools (such as, Microsoft SMS) to publish the installation of the SSL Network Extender, as an MSI package, in configuring the SSL Network Extender.

To prepare the SSL Network Extender MSI package:

1. Copy the `$FWDIR/conf/extender/extender.cab` file to a Windows machine and open the file using WinZip, or similar archive manager.
2. Extract the `cpextender.msi`, and use as an MSI package, for remote installation.

On Windows , macOS, and Linux, it is possible to install SSL Network Extender for users that are not administrators, if the user knows the admin password.

In this case, perform a regular SSL Network Extender installation and supply the administrator password when asked.

Uninstall on Disconnect

If the administrator configured **Uninstall on Disconnect** to ask the user whether or not to uninstall, the user can configure **Uninstall on Disconnect** as follows:

1. Click **Disconnect**.

   The **Uninstall on Disconnect** window appears.

2. Click **Yes** to uninstall.

   If you click **Cancel**, the SSL Network Extender is not uninstalled.

   If you click **Yes**, the **Uninstall on Disconnect** window appears the next time the user connects to the SSL Network Extender.

Troubleshooting SSL Network Extender

Below are tips on how to resolve issues that you may encounter when using SNX.

For more information, see:

- sk103572 - How to debug SSL Network Extender Client on Windows machines for Network Mode
- sk33833 - How to debug SSL Network Extender Client on Linux and macOS machines

SSL Network Extender Issues

All user's packets destined directly to the external SSL Network Extender Security Gateway are not encrypted by the SSL Network Extender.

If there is a need to explicitly connect to the Security Gateway through the SSL tunnel, connect to the internal interface, which is part of the encryption domain.

1. **The SSL Network Extender Security Gateway allows users to authenticate themselves via certificates. Therefore, when connecting to the SSL Network Extender Security Gateway, this message may appear: "`The Web site you want to view requests identification. Select the certificate to use when connecting.`"**

   To now show this message to the users, two solutions are proposed:

   a. On the client computer, open the Internet Explorer.

      Below **Tools > Options > Security** tab, select **Local intranet > Sites**.

      You can now add the SSL Network Extender Security Gateway to the Local intranet zone, where the Client Authentication pop-up does not appear.

      Click **Advanced**, and add the Security Gateway external IP or DNS name to the existing list.

   b. On the client computer, open the Internet Explorer.

      Below **Tools > Options > Security** tab, select **Internet Zone > Custom Level**. In the **Miscellaneous** section, select **Enable** for the item **Don't prompt for client certificate selection when no certificates or only one certificate exists**. Click **OK**. Click **Yes** in the confirmation window. Click **OK** again.

      Note - This solution changes the behavior of the Internet Explorer for all Internet sites, so if better granularity is required, refer to the previous solution.

2. **If the client computer has Endpoint Security VPN software installed, and is configured to work in 'transparent mode', and its encryption domain contains SSL Network Extender Security Gateway, or otherwise overlaps with the SSL Network Extender encryption domain, the SSL Network Extender does not function properly.**

   To resolve this, disable the overlapping site in Endpoint Security VPN.

3. **If the client computer has Endpoint Security VPN software installed, and is configured to work in 'connect mode', and its encryption domain contains SSL Network Extender Security Gateway, or otherwise overlaps with the SSL Network Extender encryption domain, the SSL Network Extender does not function properly.**

   To resolve this, make sure the value of the parameter "`allow_clear_traffic_while_disconnected`" is `True` (which is the default value).

vpn set_snx_encdom_groupsh

Description

This Expert mode command on the Security Gateway controls the "encryption domain per usergroup" feature for SSL Network Extender.

Syntax

```
vpn set_snx_encdom_groups
      off
      on
```

Parameters

Parameter	Description
`off`	Disables the feature.
`on`	Enables the feature.

VPN Debug

See sk180488 - How to collect a debug for VPN issues.