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.

Check Point E80.71 and Higher
For more about this release, see the E80.71 and Higher Mac client home page http://supportcontent.checkpoint.com/solutions?id=sk121595

Latest Version of this Document
Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=59843.
To learn more, visit the Check Point Support Center https://supportcenter.checkpoint.com.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security VPN for Mac E80.71 and Higher Administration Guide.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 December 2018</td>
<td>Second release of the document to include higher EPS software versions</td>
</tr>
<tr>
<td>18 December 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Overview of Endpoint Security VPN</td>
<td>6</td>
</tr>
<tr>
<td>Topology Architecture</td>
<td>6</td>
</tr>
<tr>
<td>Encryption Domains</td>
<td>7</td>
</tr>
<tr>
<td>External Resources in Encryption Domain</td>
<td>8</td>
</tr>
<tr>
<td>Setting Up Endpoint Security VPN</td>
<td>9</td>
</tr>
<tr>
<td>Installing the Endpoint Security VPN Hotfix</td>
<td>9</td>
</tr>
<tr>
<td>Required Gateway Settings</td>
<td>10</td>
</tr>
<tr>
<td>Configuring a Policy Server</td>
<td>10</td>
</tr>
<tr>
<td>Remote Access Modes</td>
<td>11</td>
</tr>
<tr>
<td>Distributing Endpoint Security VPN</td>
<td>12</td>
</tr>
<tr>
<td>Authentication Schemes and Certificates</td>
<td>12</td>
</tr>
<tr>
<td>Pre-Configuring Authentication Method</td>
<td>12</td>
</tr>
<tr>
<td>Certificates</td>
<td>13</td>
</tr>
<tr>
<td>SecurID</td>
<td>16</td>
</tr>
<tr>
<td>Challenge-Response</td>
<td>17</td>
</tr>
<tr>
<td>Authentication Timeout</td>
<td>17</td>
</tr>
<tr>
<td>Advanced Client Settings</td>
<td>17</td>
</tr>
<tr>
<td>Pre-Configuring Logging Options</td>
<td>17</td>
</tr>
<tr>
<td>Proxy Settings</td>
<td>18</td>
</tr>
<tr>
<td>Configuring Client Interface Language</td>
<td>18</td>
</tr>
<tr>
<td>Helping Your Users</td>
<td>19</td>
</tr>
<tr>
<td>Simple Installation</td>
<td>19</td>
</tr>
<tr>
<td>Endpoint Security VPN Client Icon</td>
<td>19</td>
</tr>
<tr>
<td>Helping Users Create a Site</td>
<td>20</td>
</tr>
<tr>
<td>Preparing the Gateway Fingerprint</td>
<td>20</td>
</tr>
<tr>
<td>Using the Site Wizard</td>
<td>20</td>
</tr>
<tr>
<td>Opening the Site Wizard Again</td>
<td>22</td>
</tr>
<tr>
<td>Helping Users with Basic Client Operations</td>
<td>23</td>
</tr>
<tr>
<td>Configuring Client Features</td>
<td>24</td>
</tr>
<tr>
<td>Managing Desktop Security</td>
<td>24</td>
</tr>
<tr>
<td>Installing Desktop Security Policy</td>
<td>24</td>
</tr>
<tr>
<td>The Desktop Firewall</td>
<td>24</td>
</tr>
<tr>
<td>Rules</td>
<td>25</td>
</tr>
<tr>
<td>Default Policy</td>
<td>26</td>
</tr>
<tr>
<td>Logs and Alerts</td>
<td>26</td>
</tr>
<tr>
<td>Wireless Hotspot/Hotel Registration</td>
<td>26</td>
</tr>
<tr>
<td>Planning Desktop Security Policy</td>
<td>27</td>
</tr>
<tr>
<td>Operations on the Rule Base</td>
<td>27</td>
</tr>
<tr>
<td>Desktop Security Policy in R77.x and Lower</td>
<td>27</td>
</tr>
<tr>
<td>Letting Users Disable the Firewall</td>
<td>28</td>
</tr>
<tr>
<td>Secure Configuration Verification (SCV)</td>
<td>28</td>
</tr>
<tr>
<td>Configuring Compliance Checks in Endpoint Security VPN for Mac</td>
<td>29</td>
</tr>
<tr>
<td>Required Applications and Files</td>
<td>29</td>
</tr>
</tbody>
</table>
Overview of Endpoint Security VPN

Endpoint Security VPN for Mac is a simple and secure way for endpoints to connect remotely to corporate resources over the Internet, through a VPN tunnel. It incorporates Remote Access VPN with Desktop Security in a single client. It is recommended for managed endpoints that require a simple and transparent remote access experience together with desktop firewall rules.

- This release replaces SecureClient for Mac.
- An integrated desktop firewall is centrally managed from Security Management Server.
- It requires the IPsec VPN Software Blade on the gateway, an Endpoint Container license, and the Endpoint VPN Software Blade on the Security Management Server.

See the E80.71 and Higher Release Notes http://supportcontent.checkpoint.com/solutions?id=sk119676 for a list of included features.

Topology Architecture

Endpoint Security VPN Selective Routing lets you define different encryption domains for each VPN site-to-site community and Remote Access (RA) Community. You must have a VPN domain configured. The domain includes participating gateways.

To configure selective routing:

1. In the Network Objects Tree, right click the Security Gateway and select Edit. The Check Point Security Gateway properties page opens.
2. Select Topology to display the topology window.
4. Click Set. The Set VPN Domain per Remote Access Community window opens.
5. From the drop down menu, select the object that will represent the Remote Access VPN domain.
6. Click OK.
Encryption Domains

Here are examples of ways to set up the architecture of an encryption domain.

Scenario 1: Dedicated Encryption Domain

<table>
<thead>
<tr>
<th>Component</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Gateway of Site 1</td>
<td>• Gateway of Site 2 in site-to-site VPN</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Security VPN, as their VPN gateway</td>
</tr>
<tr>
<td>2 Gateway of Site 2</td>
<td>Gateway of Site 1 in site-to-site VPN</td>
</tr>
<tr>
<td>3 Servers in Remote Access Encryption Domain</td>
<td>Servers in Encryption Domain of Site 2</td>
</tr>
<tr>
<td>4 Servers in Remote Access Encryption Domain</td>
<td>Servers in Encryption Domain of Site 1</td>
</tr>
<tr>
<td>5 Endpoint Security VPN</td>
<td>• Gateway of Site 1 through encrypted VPN</td>
</tr>
<tr>
<td></td>
<td>• Permitted servers [3]</td>
</tr>
<tr>
<td></td>
<td>• Note - cannot connect to denied servers [4]</td>
</tr>
</tbody>
</table>

Scenario 2: Access to External Encryption Domain

<table>
<thead>
<tr>
<th>Component</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Gateway of Site 1</td>
<td>• Gateway of Site 2 in site-to-site VPN</td>
</tr>
<tr>
<td></td>
<td>• Endpoint Security VPN, as their VPN gateway</td>
</tr>
<tr>
<td></td>
<td>• Relays clients to servers in other site’s encryption domain (4) through VPN</td>
</tr>
<tr>
<td>Component</td>
<td>Connects To</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2 Gateway of Site 2</td>
<td>Gateway of Site 1 in site-to-site VPN</td>
</tr>
<tr>
<td>3 Servers in Remote Access Encryption Domain</td>
<td>Servers in Encryption Domain of Site 2</td>
</tr>
<tr>
<td>4 Servers in Remote Access Encryption Domain</td>
<td>Servers in Encryption Domain of Site 1</td>
</tr>
<tr>
<td>5 Endpoint Security VPN</td>
<td>• Gateway of Site 1 through encrypted VPN&lt;br&gt;• Permitted servers (3 and 4)&lt;br&gt;Note - clients can reach servers of two sites with one authentication session, and their activity in both sites is logged</td>
</tr>
</tbody>
</table>

**External Resources in Encryption Domain**

<table>
<thead>
<tr>
<th>Component</th>
<th>Connects To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Gateway of Site 1</td>
<td>• Endpoint Security VPN, as their VPN gateway (5)&lt;br&gt;• External resource (4)&lt;br&gt;• Redirects clients (5) to external resource (4)</td>
</tr>
<tr>
<td>2 Remote Access Encryption Domain</td>
<td>Encrypted domain of gateway (1) that includes an external resource</td>
</tr>
<tr>
<td>3 Servers in Encryption Domain</td>
<td>External resource</td>
</tr>
<tr>
<td>4 External (Internet or DMZ) resource in Encryption Domain</td>
<td>• Server in Encryption Domain&lt;br&gt;• Endpoint Security VPN if the gateway redirects</td>
</tr>
<tr>
<td>5 Endpoint Security VPN</td>
<td>• Gateway of Site 1 through encrypted VPN&lt;br&gt;• Permitted servers (3)&lt;br&gt;• External resource (4), through gateway redirect</td>
</tr>
</tbody>
</table>
Setting Up Endpoint Security VPN

In This Section:

- Installing the Endpoint Security VPN Hotfix ........................................................ 9
- Required Gateway Settings .................................................................................. 10
- Configuring a Policy Server .................................................................................. 10
- Remote Access Modes ......................................................................................... 11
- Distributing Endpoint Security VPN ................................................................. 12
- Authentication Schemes and Certificates ............................................................. 12
- Advanced Client Settings ..................................................................................... 17

Endpoint Security VPN requires a supported gateway version.

See the E80.71 and Higher Release Notes http://supportcontent.checkpoint.com/solutions?id=sk119676 to see if a hotfix is required for your environment.

The initial workflow includes:

- Install the gateway Hotfix, if required.
- Configure the gateway.
- Download the client package from the Download Center.
- Distribute the client by email or other methods.

Installing the Endpoint Security VPN Hotfix

If you have R71.30 and higher or R75 and higher installed on a gateway, Security Management Server, or Multi-Domain Server, it can support Endpoint Security VPN. It is not necessary to install a Hotfix. See the System Requirements section of the Release Notes for exact details.

For earlier supported gateway versions, install the Hotfix http://supportcontent.checkpoint.com/solutions?id=sk67820.

Install the Endpoint Security VPN E80.71 and Higher Hotfix on gateways or standalone, self-managed gateway deployments. In a Multi-Domain Security Management environment install the Hotfix on the Multi-Domain Server.

Before you install the Hotfix:

This Hotfix has possible conflicts with other installed Hotfixes. If you can, it is safest to uninstall all Hotfixes installed on the Security Management Server or gateways. See Uninstalling a Hotfix. If you cannot uninstall a Hotfix, contact Check Point Technical Support.

To install the Hotfix on a Security Gateway or Security Management Server:

1. Download the Hotfix.
3. Run the Hotfix:
   On SecurePlatform, Disk-based IPSO, and Solaris:
   a) tar -zxvf <name_of_file>.tgz
   b) ./UnixInstallScript
   On Windows platforms: double-click the installation file and follow the instructions.

To install the Hotfix on a Multi-Domain Server:
2. Download the Endpoint Security VPN Hotfix to the Multi-Domain Server.
3. Run the Hotfix on SecurePlatform and Solaris:
   a) tar -zxvf <name_of_file>.tgz
   b) ./UnixInstallScript
4. Follow the on-screen instructions.
5. Reboot the Multi-Domain Server.

Required Gateway Settings
You must configure one or more Security Gateways to work with Endpoint Security VPN. These procedures are necessary for Endpoint Security VPN operations.

Note - The procedures shown are for R77.x and R80.x gateways. For other versions, the exact procedure might be slightly different.

For more information about the options in the procedures, see the VPN documentation for your gateway version:
- **VPN Remote Access Administration Guide** (R80.10 and higher)
- **VPN Administration Guide** (Pre- R80)

Configuring a Policy Server
The Policy Server functionality in a gateway is the Desktop Security Policy management. If you do not enable a Policy Server, the Desktop rule base is not applied.

To define a gateway as the Policy Server:
1. In SmartDashboard, right-click the gateway that will serve as the Policy Server and select Edit.
   The Check Point Gateway window opens.
2. Enable Policy Server functionality:
   - R70 and higher: In **Software Blades > Network Security**, click **IPSec VPN** and **Policy Server**.
   - NGX R65: In **Check Point Products**, click **VPN** and **SecureClient Policy Server**.
3. Open Authentication.

![Authentication settings](image)

4. From the Users drop-down, select an existing user group of remote access clients. Users that authenticate to the gateway must belong to this group.

5. Click OK.

Remote Access Modes

In the Remote Access page of a gateway, you can configure Visitor Mode and Hub Mode. Visitor Mode is required. Hub Mode is optional. In Hub Mode, the gateway is the VPN router for clients. All connections that the client opens are passed through the gateway, even connections to the Internet.

In E80.70 and higher you can exclude local networks when Hub Mode is enabled.

*Note* - Hub mode is not supported in SecuRemote.

To enable Hub Mode:

1. Open Global Properties:
   - R77.x - In SmartDashboard, open File > Policy > Global Properties.
   - R80.x - In SmartConsole, open Menu > Global Properties
2. Open Remote Access > Endpoint Connect.
3. Select an option in Security Settings > Route all traffic to gateway:
   - *No* - Clients route only VPN traffic through the gateway. Traffic from the client to public sites is not routed. This is default. It prevents adverse performance on the gateway due to heavier loads.
   - *Yes* - The clients use Hub Mode and the user cannot change this.
   - *Configured on endpoint client* - Clients that you pre-configure to use VPN Tunneling will use Hub Mode and the user cannot change this setting. Clients that you do not pre-configure for VPN Tunneling will use the setting that users choose.
Distributing Endpoint Security VPN

When you distribute the client to users, make sure that they have:

- **VPN site information** - Users will have to create the site the first time they connect to it. Make sure they have the IP address or hostname of the VPN site.

- **Authentication Information** - Users will have to select an authentication method and have the supplies required for that authentication method. For example, if users authenticate with certificates, make sure they have the certificate file before connection. Make sure they know that they must not delete this file.

You can configure a default authentication method for a site in the gateway configuration file (on page 12).

You can distribute the installation file to users in different ways, for example, by email.

Authentication Schemes and Certificates

To create a secure connection to the LAN from a remote location, users must authenticate themselves.

Endpoint Security VPN supports these authentication types:

- Username and password
- Certificate - Keychain (for Keychain certificates and Smart Cards)
- Certificate - P12
- SecurID - KeyFob
- SecurID - PinPad
- Challenge Response

Pre-Configuring Authentication Method

From the client, users can change how they authenticate to a VPN gateway. You can pre-configure the default authentication method in the gateway configuration file.

**To configure default authentication for users of a site:**

1. On the gateway, open the $FWDIR/conf/trac_client_1.ttm file with a text editor.
2. In the `default_authentication_method` section, change :default
   Valid values:
   - client_decide (let user decide, default)
   - username-password
   - certificate (for Keychain certificate)
   - p12-certificate
   - securIDKeyFob
   - securIDPinPad
   - challenge-response
3. Save the file and install the policy.

   When clients download the new policy from the gateway, configuration changes are applied.
This example shows a configuration for Certificate - P12 authentication.

```
:default_authentication_method {
    :gateway {
        :map {
            :username-password (username-password)
            :challenge-response (challenge-response)
            :certificate (certificate)
            :p12-certificate (p12-certificate)
            :securIDKeyFob (securIDKeyFob)
            :securIDPinPad (securIDPinPad)
            :SoftID (SoftID)
            :SAA-username-password (SAA-username-password)
            :SAA-challenge-response (SAA-challenge-response)
            :client_decide (client_decide)
        }
        :default (p12-certificate)
    }
}
```

Users who define the site for this gateway are not prompted to select an authentication method.

### Certificates

A certificate is a digital ID card. It is issued by a trusted third party known as a Certification Authority (CA). Endpoint Security VPN can use the digital certificates issued by the gateway, which has its own Internal Certificate Authority (ICA). A digital certificate has:

- User name.
- A serial number.
- An expiration date.
- A copy of the public key of the certificate holder (used to encrypt messages and digital signatures).
- The digital signature of the certificate-issuing authority, in this instance the ICA. This lets the gateway confirm that the certificate is valid.

### Stored in Keychain or Stored as Files

Endpoint Security VPN support user authentication through PKCS#12 certificates. A PKCS#12 certificate can be accessed directly when stored as a .p12 file or imported to the Keychain store.

The Keychain is used to store and access Smart Cards stored on file. For Smart Cards, you must install the correct token driver from the Smart Card middleware vendor.

**Decide whether to let users import certificates to the Keychain store:**

- Certificates in the Keychain store are easier to manage.
- If a user has several computers, will use a temporary computer, or is using a laptop [that might be stolen], it is better if the certificate is not stored on the computer. Give the user a PKCS#12 certificate on removable media.
Generating and Deploying Certificates

Generate certificates in SmartDashboard:

- **Enroll Certificate (Generate Registration Key).** Initiate a certificate that will be pending for the user. The result is a registration key. The user completes the creation of the certificate with the registration key. The result can be a certificate stored as a PKCS#12 file or stored in the Keychain.

- **Generate PKCS#12 File.** Generate a PKCS#12 certificate and save it to a file. The user authenticates with the PKCS#12 file.

Generating Registration Keys

Generate a registration key from SmartDashboard to let users import certificates to the Keychain store.

To generate a registration key:

1. In SmartDashboard, click Manage menu > Users and Administrators.
   - The Users and Administrators window opens.
2. Select one user and click Edit.
   - The User Properties window opens.
3. Open Certificates.
4. Click Initiate.
   - The registration key is generated. Give it to the user.
   - The registration key has an expiration date. If the user does not complete the task before the expiration date, the registration key is deleted.

Generating PKCS#12 Files

Generate a certificate file from SmartDashboard.

To generate a certificate file:

1. In SmartDashboard, click Manage menu > Users and Administrators.
   - The Users and Administrators window opens.
2. Select one user and click Edit.
   - The User Properties window opens.
3. Open Certificates.
4. Click Generate and save.
5. Let the user choose and confirm a password.
6. Save the certificate to a file.
   - The certificate file is generated. Give it to the user.

Certificate Enrollment and Renewal

A. To enroll a certificate:

1. Click the client icon in the menu bar, and select VPN Options.
2. On the Sites tab, select the site from which you will enroll a certificate and click Properties.
   - The site Properties window opens.
3. Select the **Settings** tab.
4. Choose the setting type you want, Keychain or P12, and click **Enroll**.
   The **Keychain** or **P12** window opens.
5. For Keychain, choose the keychain to which you will enroll the certificate.
6. For P12, choose a new password for the certificate and confirm it.
7. Enter the Registration Key that your administrator sent you.
8. Click **Enroll**.
   The certificate is enrolled and ready for use.

**B. To renew a certificate:**
1. Click the client icon in the menu bar, and select **VPN Options**.
2. On the **Sites** tab, select the site from which you will renew a certificate and click **Properties**.
   The site **Properties** window opens.
   The authentication method you chose is set and the certificate will be renewed accordingly.
3. Select the **Settings** tab.
4. Click the **Renew** button.
   The **Keychain** or **P12** window opens.
5. For Keychain, choose the certificate you want to renew from the drop-down list. For P12, choose a P12 file and enter its password.
6. Click **Renew**.
   The certificate is renewed and ready for use.

**Revoking Certificates**
If you need to block a user from connecting, revoke the certificate. The user will not be able to authenticate to the VPN.

To revoke a certificate, in SmartDashboard, in the **User Properties** window > **Certificates**, click **Revoke**.

**Helping Users Import Certificates**
If you give users a certificate to keep on the computer, you can help them import the certificate to the Keychain store. Make sure that users have the file itself, or access to it, and that they have the password for the certificate.

To import a certificate through the client:
1. Click the client icon in the menu bar, and select **VPN Options**.
2. On the **Sites** tab, select the gateway and click **Properties**.
3. Open the **Settings** tab.
4. Make sure that **Certificate - Keychain** is selected in the **Method** menu.
5. Click **Import**.
7. Enter the certificate password and click **Import**.
To import a certificate through Finder:
1. Double-click the P12 file.
   The Keychain application opens and a prompt shows for the certificate password.
2. Enter the certificate password.

Disabling Certificate Authentication

Endpoint Security VPN support user authentication with PKCS#12 certificates. A PKCS#12 certificate can be accessed directly or imported to the Keychain store.

If you do not want users to authenticate with certificates stored in the Keychain store:

1. On the gateway, open the $FWDIR/conf/trac_client_1.ttm file.
2. Change the :default attribute, located in the enable_capi section, to false.

   ```
   enable_capi (
     :gateway (
       :map (
         :false (false)
         :true (true)
         :client_decide (client_decide)
       )
       :default (false)
     )
   )
   ```
3. Save the file and install the policy.
   When clients download the new policy from the gateway, configuration changes are applied.

SecurID

The RSA SecurID authentication mechanism consists of hardware (FOB, USB token) that generates an authentication code at fixed intervals (usually one minute), with a built-in clock and encoded random key.

The most common form of SecurID Token is the hand-held device. The device is usually a key FOB or slim card. The token can have a PIN pad, onto which a user enters a personal identification number (PIN) to generate a passcode. When the token does not have a PIN pad, a tokencode is displayed. A tokencode is the changing number displayed on the key FOB.

Endpoint Security VPN uses both the PIN and tokencode, or just the passcode, to authenticate to the gateway.

Key Fobs

A key fob is a small hardware device with built-in authentication mechanisms that control access to network services and information. While a password can be stolen without the owner realizing it, a missing key fob is immediately apparent. Key fobs provide the same two-factor authentication as other SecurID devices. The user has a personal identification number (PIN), which authenticates that person as the owner of the device; after the user enters the correct PIN, the device displays a number which allows the user to log on to the network. The SecurID SID700 key fob is a typical example of such a device.
Working with RSA Tokens

If you use SecurID for authentication, you must define users on an RSA ACE management server. You must also add SecurID users to a group with an external user profile account that includes SecurID as the Authentication Method.

See the SecureID RSA documentation of how to configure RSA with Check Point gateways.

Challenge-Response

Challenge-response is an authentication protocol in which one party provides the first string (the challenge), and the other party verifies it with the next string (the response). For authentication to take place, the response is validated.

Authentication Timeout

Authentication Timeout is how long a client password is valid before the user must enter it again. By default, this is one day.

To change Authentication Timeout:

1. On SmartDashboard, open the Global Properties window > Remote Access page.
2. In Authentication Timeout, select Validation timeout every and enter a value in minutes.

Advanced Client Settings

Configure client behavior in the VPN Options > Advanced tab.

1. Click the client icon in the menu bar, and select VPN Options.
   The Options window opens.
2. Open the Advanced tab.

Pre-Configuring Logging Options

Users can send log files with their default email account. You can configure the client for your email address.

To define a default email address for log files:

1. Open $FWDIR/conf/trac_client_1.ttm on the gateway.
2. Enter a default email address in the send_client_logs attribute.

```plaintext
:send_client_logs (    :gateway (      :default ("email@example.com")    )
)
```

If no default email address is defined, users can click Collect Logs in the Options > Advanced window of the Endpoint Security VPN client. This action stores all client logs in a single CAB file, which users can send to you for troubleshooting.

3. Save the file and install the policy.
   When clients download the new policy from the gateway, configuration changes are applied.
Proxy Settings

Note - Remote-location proxy-server settings are usually detected automatically.

If a user is at a remote site that has a proxy server, the client must be configured to pass through the proxy server to reach the gateway.

You can help your user configure the proxy server when the issue comes up.

To configure proxy settings on the client:

1. In the Options > Advanced tab, click Proxy Settings.
   The Proxy Settings window opens.

2. Select an option.
   - No proxy - default
   - Detect proxy from System Preferences settings - When this option is selected, the Client uses proxy settings as defined in your System Preferences.
     To see the settings there, select: System Preferences > Network > Advanced > Proxies.
     Note - These protocols are supported by Proxy Detection in your System Preferences settings:
     • Auto Proxy Discovery
     • Automatic Proxy Configuration
     • Web Proxy (HTTP)
   - Manually define proxy - If the proxy settings cannot be automatically detected, enter the IP address and port number of the proxy as supplied by your system administrator.

3. Click OK.

Configuring Client Interface Language

If a user wants a different language for the interface of the client, you can help them select another language.

To change the interface language:

1. Open the Options > Advanced tab.

2. From the Choose the interface language drop-down menu, select the language you want.
Helping Your Users

In This Section:
- Simple Installation ........................................................................................................ 19
- Endpoint Security VPN Client Icon ............................................................................... 19
- Helping Users Create a Site .......................................................................................... 20
- Helping Users with Basic Client Operations ............................................................... 23

This chapter is a summary of basic actions that end-users do when they install and use Endpoint Security VPN.

Simple Installation

Users can easily install Endpoint Security VPN on a supported computer without a reboot after installation.

To install Endpoint Security VPN, users do this:
1. Download the DMG package and execute it with a double-click.
2. Click Next to start.
3. Accept the agreement.
4. Click Install.
5. Click Finish.

When installation is complete, the Endpoint Security VPN icon appears in the menu bar.

Endpoint Security VPN Client Icon

The Endpoint Security VPN client icon shows the status of the client.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Disconnected]</td>
<td>Disconnected</td>
</tr>
<tr>
<td>![Connecting]</td>
<td>Connecting</td>
</tr>
<tr>
<td>![Connected]</td>
<td>Connected</td>
</tr>
<tr>
<td>![Encryption]</td>
<td>Encryption (encrypted data is being sent or received on the VPN)</td>
</tr>
<tr>
<td>![Issue]</td>
<td>There is an issue that requires users to take action.</td>
</tr>
</tbody>
</table>
Helping Your Users Create a Site

Each client must have at least one site defined. The site is the VPN gateway. Make sure your users have:

- The gateway fingerprint.
- The gateway IP address or domain name.
- The authentication method that they will use.
- Authentication materials (username, password, certificate file, RSA SecurID, or access to Help Desk for challenge/response authentication).

Preparing the Gateway Fingerprint

Before users define a site that leads to the gateway, prepare the fingerprint of the gateway. Users may get a warning that the client cannot identify the gateway and that they should verify the fingerprint.

Give the users the fingerprint to compare with their client installation and site definition.

To prepare the gateway fingerprint:

1. In SmartDashboard, click Manage menu > Servers and OPSEC Applications.
2. In the Servers and OPSEC Applications window, select the Certificate Authority and click Edit.
3. Open the Local Security Management Server or OPSEC PKI tab and click View.
4. In the Certificate Authority Certificate View window, copy the SHA Fingerprint.
5. Send the fingerprint to users before they install the client.

For R80.10 and higher gateways, do the procedure above from the legacy SmartDashboard.

To open the legacy SmartDashboard from R80.x SmartConsole:

1. In SmartConsole go to the Security Policies view.
2. Under Shared Policies, click Mobile Access or DLP.
3. Click Open Policy in SmartDashboard.

Using the Site Wizard

When the user first double-clicks the Endpoint Security VPN icon, a message opens:

No site is configured. Would you like to configure a new site?

- If the user clicks No, the message closes. The user cannot connect to a VPN until a site is defined.
- If the user clicks Yes, the Site Wizard opens.
To configure the first site of a client:

1. The user clicks **Next**.
2. The user enters the IP address or name of the VPN gateway.
   - If a DNS server is configured and the client is within the internal network, the client detects the VPN site automatically.

```
<table>
<thead>
<tr>
<th>Server address or Name:</th>
<th>example.domain.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name:</td>
<td>My Gateway</td>
</tr>
</tbody>
</table>
```

The wizard shows the progress while the Client resolves the site name or address to the actual gateway. This step in the wizard notifies the user that:
- This may take several minutes, depending on the speed of your network connection.

If users see the certificate warning, make sure they check the fingerprint of the gateway:

a) Compare the site fingerprint with the SIC fingerprint on the gateway.

b) Click **Details** to see additional warnings.

c) If site details are correct, click **Trust and Continue**. The fingerprint is stored internally and the security warning is not opened again for the site, even if the client is upgraded.
The wizard displays the authentication method step.

![Authentication Method](image)

**Authentication Method**
Select the authentication method to be used.

- **Username and Password**
  Click if your system administrator provided you with account name and a password.

- **Certificate**
  If you are using Hardware tokens or any other certificate type.

- **SecurID**
  Click if you are using RSA SecurID.

- **Challenge Response**
  Click if you are required to provide different responses to a challenge

3. Give your users the authentication materials they need.
4. The user selects the correct method and clicks **Next**.
   - If **Certificate**, the user selects **PKCS#12** or **Keychain** (make sure the user knows which to select), and clicks **Next**.
   - If **SecurID**, the user selects the type, and clicks **Next**.
5. The user clicks **Finish** and a message shows: Would you like to connect?
   If the user clicks **Yes**, the client connects to the gateway and a VPN tunnel is created.

### Opening the Site Wizard Again

The Site wizard opens automatically the first time a client is opened. You can also open it at any time.

**To create a new site on the client at any time:**

1. Click the client icon and select **VPN Options**.
   The Options window opens.
2. On the **Sites** tab, click **New.**
   The Site Wizard opens.
   
   OR

3. Click the client icon and select **Connect to.**

4. In the **Site** drop-down, select **New Site.**
   The Site Wizard opens.

### Helping Users with Basic Client Operations

Users can do basic client operations from the client icon. Click the icon and select a command.

⚠️ **Note** - The options available from the client icon differ based on the client status and configuration.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect</td>
<td>Opens the main connection window, with the last active site selected. If the user authenticates with a certificate, the client immediately connects to the selected site.</td>
</tr>
<tr>
<td>Connect to</td>
<td>Opens the main connection window.</td>
</tr>
<tr>
<td>VPN Options</td>
<td>Opens the <strong>Options</strong> window to set a proxy server and choose an interface language.</td>
</tr>
<tr>
<td>Shutdown Client</td>
<td>Closes the Client. An open VPN is closed. A background daemon continues to run. To stop the daemon, run: <code>sudo launchctl stop com.checkpoint.epc.service</code>. If you close Endpoint Security VPN and stop the service, the desktop firewall still enforces the security policy.</td>
</tr>
</tbody>
</table>
Managing Desktop Security

Desktop Security is the firewall policy for remote access clients. Configure it in the Desktop tab in SmartDashboard.

Installing Desktop Security Policy

To install the Desktop Security policy (for SmartConsole-managed Endpoint Security VPN only):

1. Click Install Policy.
2. In the Install Policy window, select Desktop Security for the Endpoint Security VPN gateway.
   If this column is not available, you did not configure the Policy Server. This is necessary. See Configuring a Policy Server (on page 10).
3. Click OK.
   When clients download the new policy from the gateway, configuration changes are applied.

The Desktop Firewall

Endpoint Security VPN enforces a Desktop Security Policy on remote clients. You define the Desktop Security Policy in a Rule Base. Rules can be assigned to specific user groups, to customize a policy for different needs.

⚠️ Important - Before you begin to create a Desktop Security Policy, you must enable the Policy Server feature on the gateway.

Endpoint Security VPN downloads the first policy from the gateway. It looks for and downloads new policies every time it connects or on re-authentication.
When Endpoint Security VPN makes a VPN connection, it connects to the gateway and downloads its policy. Endpoint Security VPN enforces the policy: accepts, encrypts, or drops connections, depending on their source, destination, and service.

### Endpoint Security VPN Desktop Policy Architecture

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Management Server</td>
<td>Manages all policies</td>
</tr>
<tr>
<td>2</td>
<td>Gateway</td>
<td>Firewall of LAN, holds Desktop Security Policy and TTM configuration</td>
</tr>
<tr>
<td>3</td>
<td>Endpoint Security VPN client</td>
<td>Gets Desktop Security Policy from gateway and enforces policy on client computer</td>
</tr>
</tbody>
</table>

### Rules

The Desktop Security Policy has Inbound and Outbound rules.

- **Inbound rules** - enforced on connections going to the client computer.
- **Outbound rules** - enforced on connections originating from the client computer.

Each rule defines traffic by source, destination, and service. The rule defines what action to take on matching traffic.

- **Source**: The network object which initiates the communication.
- **Destination**: The user group and location for Inbound communications, or the IP address of Outbound communications.
- **Service**: The service or protocol of the communication.
- **Action**: **Accept**, **Encrypt**, or **Block**.

### Implied Rules

The Desktop Security Policy has implicit rules appended to the end of inbound and outbound policies.

- The implicit **outbound** rule allows all connections originating from the client to go out, if they do not match previous blocking rules: **Any** Destination, **Any** Service = **Accept**.
- The implicit **inbound** rule blocks all connections coming to the client that do not match previous rules. **Any** Source, **Any** Service = **Block**.
User Granularity

You can define different rules for remote users based on locations and user groups.

- **Locations** - Set rules to be implemented by physical location. For example, a user with a laptop in the office building will have a less restrictive policy than when the same user on the same laptop connects from a public wireless access point.

- **User Groups** - Set rules to be implemented for some users and not others. For example, define restrictive rules for most users, but give system administrators more access privileges. Rules are applied to user groups, not individual users. Endpoint Security VPN does not inherently identify user groups, so it must obtain group definitions from the gateway. The gateway resolves the user groups of the authenticated user and sends this information to the Endpoint Security VPN client. Endpoint Security VPN enforces the rules applicable to the user, according to groups.

Rules can also be applied to radius groups on the RADIUS server.

Default Policy

If an Endpoint Security VPN client is disconnected from the gateway, the client enforces a default policy. This policy is enforced until Endpoint Security VPN connects to the gateway and enforces an updated personalized policy.

The default policy is taken from the last Desktop Firewall policy that was downloaded from the gateway. It includes the rules that apply to the **All Users** group. Rules from the Desktop Firewall policy that apply to other groups or users are not part of the default policy.

Logs and Alerts

Desktop Security log messages are saved locally on the client system in:

/Library/Application Support/Checkpoint/Endpoint Connect/trac_fwpktlog.log

Wireless Hotspot/Hotel Registration

Wireless hotspot is a wireless broadband Internet access service available at public locations such as airport lounges, coffee shops, and hotels.

The user launches a web browser and attempts to connect to the Internet. The browser is automatically redirected by the hotspot server to the Hotspot welcome page for registration. In the registration process, the user enters the required information. When registered, the user gains access to the Internet.

This feature supports users with restrictive outbound policies or with Hub Mode (everything goes through the Security Gateway), or both. Therefore, even if users connect to a gateway for all Internet communication, they can still access the hotspot to register.

A proxy might be required.
Planning Desktop Security Policy

Balance considerations of security and convenience. A policy should permit desktop users to work as freely as possible, but also reduce the threat of attack from malicious third parties.

- In the Inbound policy, allow only services that connect to a specific server running on the relevant port.
- In the Outbound policy, use rules to block only specific problematic services (such as Netbus), and allow all others.
- Remember: Implied rules may allow or block services not explicitly handled by previous rules. For example, if the user runs an FTP server, the inbound rules must explicitly allow connections to the FTP server.

Operations on the Rule Base

Define the Desktop Security Policy. Rules are managed in order: what is blocked by a previous rule cannot be allowed later. The right-click menu of the Rule Base is:

- Add - Add a rule above or below the selected rule.
- Disable - Rules that are currently not implemented, but may be in the future, can be disabled.
- Delete - Delete rules which are no longer necessary.
- Hide - Hide rules that are irrelevant to your current view, to enhance readability of your Rule Base. Hidden rules are still applied.
- Where Used - See where the selected network object is included in other rules.
- Show - Show the selected object or rule in SmartMap.

Desktop Security Policy in R77.x and Lower

To create a Desktop Security Policy with R77.x or lower Security Management:

1. In SmartDashboard, open the Desktop tab.
   You might need to click More to see the Desktop tab.
2. Configure the rules: Click in the Inbound Rules or Outbound Rules section and click an Add Rule icon to add a new rule.
   For each rule, include users for whom the rule applies.
   In inbound rules, Desktop (Endpoint Security VPN) is the destination.
   In outbound rules, Desktop is the source.
3. Install the policy (Policy menu > Install).
   Install the Desktop security policy on the gateways that are configured to handle Endpoint Security VPN traffic.
**Making a Rule for FTP**

If clients will use active FTP, you must add a rule to the Desktop Security Policy to specifically allow the service that you need. The service should be one of the active FTP services - anything that is not ftp-pasv.

**To add the Active FTP Rule:**

1. In SmartDashboard, open the Desktop tab.
2. Right-click the Outbound rules and select Add.
3. In the rule, select one of the FTP services as the service and Allow as the action.

**Letting Users Disable the Firewall**

You can configure if Endpoint Security VPN users can choose to disable the firewall policy on their local machines.

If this option is enabled, when users right-click the Endpoint Security VPN icon, they can select Disable Security Policy.

**To change the Allow disable firewall setting:**

1. On the gateway, open the $FWDIR/conf/trac_client_1.ttm file with a text editor.
2. Find the line :allow_disable_firewall and set the value:
   - true - Users can disable their firewall policy.
   - false - Users do not have the option to disable their firewall policy.
   - client_decide - Takes the value from a file on the client machine
3. Save the file and install the policy.

**Secure Configuration Verification (SCV)**

SCV is not supported in this release. If a gateway blocks traffic that is not compliant with SCV, you can edit the Security Management Server to allow traffic from Mac clients. To do this, configure the SCV configuration file on the Security Management Server to allow traffic from clients that do not support SCV.

**To configure the gateway to allow traffic from Mac clients:**

2. In the SCVGlobalParams section, add:
   
   ```
   :allow_non_scv_clients (true)
   ```

3. Save the file.

An alternative to SCV is to use the Endpoint Security for Mac clients Compliance blade. This is only supported when Endpoint Security VPN is installed as part of the Endpoint Security suite.
Configuring Compliance Checks in Endpoint Security VPN for Mac

To configure Endpoint Security VPN for Mac to use Endpoint Security Compliance checks:

- Configure SCV enforcement on the VPN gateway.
- Configure the VPN Client to use verifications based on Compliance checks.

To configure SCV enforcement for the Gateway:

1. In SmartDashboard, select Policy > Global Properties.
3. Select Apply Secure Configurations on Simplified Mode.
4. In the Upon Verification failure area, set the action of the gateway if a client fails one or more SCV checks and is non-compliant: Block client's connection.
5. Create a rule in the Firewall Rule Base that has the RemoteAccess VPN community object in the VPN column.
6. Click OK.
7. Open the VPN gateway object.
10. Create a default rule in the Inbound Rules with these values:

<table>
<thead>
<tr>
<th>Source</th>
<th>Desktop</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>All Users</td>
<td>Any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

11. Install the policy.

To configure the VPN Client to use verifications based on Compliance checks:

1. In SmartEndpoint, select Policy > Compliance blade.
2. Select VPN Client verification process will use Endpoint Security Compliance.
3. Install the policy.
4. Restart the client computer.

Note - If a configured verification fails, the Endpoint Security client becomes non-compliant and will not be able to access the encryption domain.

Required Applications and Files

Required Application and File Compliance Settings look for the presence of specified files, registry values, and processes that must be running or present on endpoint computers. The default settings show in the Required Application Action Rules.

For Required Application action rules, multiple check objects in the rule are mutually exclusive. If one or more check object is not compliant, the defined action and remediation is triggered.

See Compliance Action Rules for more information.
Multiple Entry Point (MEP)

Multiple Entry Point (MEP) gives high availability and load sharing to VPN connections. A gateway is one point of entry to the internal network. If the Security Gateway becomes unavailable, the internal network is also unavailable. A Check Point MEP environment has two or more Security Gateways for the same VPN domain to give remote users uninterrupted access.

MEP topology gives High Availability and load sharing with these characteristics:

- There is no physical restriction on the location of MEP gateways. They can be geographically separated and not directly connected.
- In Manual MEP gateways can be managed by different management servers. For Implicit MEP, gateways must have the same management server.
- There is no state synchronization in MEP. If a gateway fails, the current connection falls and one of the auxiliary gateways picks up the next connection.
- Remote clients, not the gateways, find the gateway to use.

Configuring Entry Point Choice

Configure how the client will choose a gateway from the multiple entry points.

- **First to Respond** - The first gateway to reply is chosen and the VPN tunnel is between that gateway and the client. The client asks for a response for each connection.
  Recommendation: If you have multiple gateways that are geographically distant. For example, an organization has three gateways: London, Sundsvall, and Paris. Usually, the London gateway responds first to clients in England and is their entry point to the internal network. If the London gateway goes down, these users access the network through the Paris or Sundsvall gateway that responds first.

- **Primary-Backup** - One or multiple auxiliary gateways give high availability for a primary gateway. Clients are configured to connect with the primary gateway, but change to a Backup gateway if the Primary goes down.
  Recommendation: If you have multiple gateways, and one is stronger or connects faster, set the stronger machine as the primary. Clients use the backup if the primary is unavailable.

- **Load Distribution** - Clients randomly select a gateway.
  Recommendation: If you have multiple gateways of equal performance. The traffic of the clients is shared between the gateways. Each client creates a tunnel with a random, available gateway.

- **Geo-Cluster DNS Name Resolution** - You can enable Geo-Clustering instead of MEP, however we recommend MEP as it is easier to manage and gives better performance. Geo-Cluster resolves gateway DNS names based on location.
Manual MEP

For implicit MEP (the method used by SecureClient), the gateways have to belong to the same VPN domain for MEP to function. For Endpoint Security VPN, if they are configured with Manual MEP, the gateways do not have to belong to the same VPN domain. Configure the TTM file of each gateway.

To configure the gateways for MEP:

1. On a gateway, open `$FWDIR/conf/trac_client_1.ttm`.
2. Search for the `enable_gw_resolving` attribute:
   ```
   :enable_gw_resolving {
     :gateway {
       :default (true)
     }
   }
   ```
3. Make sure the attribute is set to its default value: `true`.
4. Search for the `automatic_mep_topology` attribute, and make sure its value is `false`.
5. Manually add the `mep_mode` attribute:
   ```
   :mep_mode {
     :gateway {
       :default (xxx)
     }
   }
   ```
   Where `xxx` is a valid value:
   - `first_to_respond`
   - `primary_backup`
   - `load_sharing`
   - `dns_based` - Use this to configure Geo-Clusters.
6. Manually add the `ips_of_gws_in_mep` attribute:
   ```
   :ips_of_gws_in_mep {
     :gateway {
       :default (192.168.53.220)&#192.168.53.133&
     }
   }
   ```
   These are the IP addresses the client should try.
   - IP addresses are separated by an ampersand and hash symbol `&#`
   - The last IP address in the list has a final `&#`.
7. Save the file.
8. Install the policy.

Making a Desktop Rule for MEP

To use MEP, traffic to multiple sites in the encryption domain must be allowed. But the Desktop Policy sets the main site as the default Destination for outbound traffic. You must make sure that your policy allows traffic to the gateways in the encryption domain.

To add the MEP Rule:

1. In SmartDashboard, open the Desktop tab.
2. In Outbound rules, add a new rule:
   - **Destination** - a Group network object that contains all gateways in the encryption domain.
• **Service** - the Visitor Mode service (default is 443), the NAT-T port (default is 4500 UDP), and HTTP.

• **Action** - Allow.

3. Install the Policy.

### Split DNS

The Split DNS feature lets the Endpoint Security VPN client use multiple DNS servers:

- A regular DNS server for resolving the external resources.
- An internal company DNS server assigned by the Office Mode for resolving the internal company resources.

By default, the Split DNS feature is disabled in the Endpoint Security VPN client.

To configure Split DNS in the Endpoint Security VPN client:

1. Configure your VPN Gateway to assign internal company DNS Servers for Office Mode.

**To configure your VPN Gateway to assign internal DNS Servers for Office Mode:**

1. In SmartConsole or SmartDashboard, open the VPN Security Gateway object.
2. Go to **VPN Clients > Office Mode**.
3. Click **Optional Parameters**.
4. In the **DNS Servers** section, configure the internal DNS Servers.
5. In the **DNS suffixes** field, enter your internal domain names.
   - The Endpoint Security VPN client uses these DNS suffixes to determine which resources are internal.
6. Click **OK**.
7. Install the policy on the VPN Gateway.

**To configure Split DNS locally in the Endpoint Security VPN client:**

1. Log in to the Endpoint Security VPN client computer with administrator privileges.
2. Edit this file in a plain text editor:
   ```
   /Library/Application Support/Checkpoint/Endpoint Security/Endpoint Connect/trac.defaults
   ```
3. Find the attribute `split_dns_for_mac`.
4. Set the desired attribute value:
   - `false` (default) - The Endpoint Security VPN client disables the Split DNS.
   - `true` - The Endpoint Security VPN client enables the Split DNS.
5. Save the changes in the file and close the text editor.
6. Go to the **Applications** folder > **Utilities** folder.
7. Open the **Terminal** application.
8. Restart the Check Point Endpoint Security VPN client service. Run:
   ```
   sudo launchctl stop com.checkpoint.epc.service
   sudo launchctl start com.checkpoint.epc.service
   ```
To configure Split DNS from the VPN Gateway:

**Note** - These steps affect all Endpoint Security VPN clients that connect to this VPN Gateway.

1. Connect to the command line on the VPN Gateway.
2. Log in to Expert mode.
3. Create a backup copy of the $FWDIR/conf/trac_client_1.ttm file:
   ```bash
   cp -v $FWDIR/conf/trac_client_1.ttm{,_bkp}
   ```
4. Edit the $FWDIR/conf/trac_client_1.ttm file in a plain text editor:
   ```bash
   vi $FWDIR/conf/trac_client_1.ttm
   ```
5. Add the `split_dns_for_mac` property to the file in this format:
   ```bash
   :split_dns_for_mac ( 
   :gateway ( 
   :map ( 
   :true (true) 
   :false (false) 
   :client_decide (client_decide) 
   ) 
   :default (your desired value) 
   ) 
   )
   ```
6. Set the desired value for the `:default` attribute:
   - `true` - The Endpoint Security VPN client enables the Split DNS.
   - `false` - The Endpoint Security VPN client disables the Split DNS.
   - `client_decide` (default) - The Endpoint Security VPN client configures the Split DNS based on the value of the attribute `split_dns_for_mac` in its local file `/Library/Application Support/Checkpoint/Endpoint Security/Endpoint Connect/trac.defaults. See the procedure *To configure Split DNS locally in the Endpoint Security VPN client* above.
7. Save the file and close the text editor.
8. In SmartConsole or SmartDashboard, install the policy on the VPN Gateway.
9. Configuration changes are applied when the Endpoint Security VPN client connects to the VPN Gateway and downloads the new policy.

**Global Properties for Endpoint Security VPN Gateways**

Many Endpoint Security VPN properties are centrally managed on the server, rather than per gateway or per client.

To configure Endpoint Security VPN features in Global Properties:

1. Open SmartDashboard.
2. Open *Policy > Global Properties.*

4. Set Authentication Settings (on page 34).
5. Set Connectivity Settings.
   - Connect Mode (on page 35)
   - Disconnect when device is idle (on page 35)
7. Set Client upgrade mode.
8. Click OK.
9. Install the policy.

Authentication Settings

In Authentication Settings of Global Properties > Remote Access > Endpoint Connect, you can enable a password cache and define timeouts for password retention and re-authentication.

To configure authentication settings:

- **Enable password caching**
  - No (default) requires users to enter a password whenever they connect.
  - Yes retains the user password in a cache for a specified period.

- **Cache password for** - Password retention period in minutes (default = 1440), if password caching is enabled.
Note - For security reasons, the cache is cleared when the user explicitly disconnects, even if the cache period has not ended. The cache is useful for re-authentications and automatic connections triggered by the Always-Connect feature.

- **Re-authenticate** - Authentication timeout in minutes (default = 480), after which users must re-authenticate the current connection.

- **Caching and OneCheck User Settings** - In SmartEndpoint-managed clients, if you have OneCheck User Settings enabled, see the OneCheck User Settings in the *Endpoint Security Administration Guide*.

### Connect Mode

In the **Connectivity Settings** of **Global Properties > Remote Access > Endpoint Connect**, configure how clients connect to the gateway.

- **Manual** - VPN connections are not initiated automatically. Users select a site and authenticate every time they need to connect.

- **Always connected** - Endpoint Security VPN will automatically establish a connection to the last connected gateway. This is also known as **always-connect** mode.

- **Configured on endpoint client** - Connection method is set by each Endpoint Security VPN client. In the client, this is configured on **Sites > Properties > Settings**.

### Idle VPN Tunnel

Typically, VPN tunnels carry work-related traffic. To protect sensitive data and access while a remote access user is away from the machine, make sure that idle tunnels are disconnected.

To configure tunnel idleness:

2. Open the **Global Properties > properties > firewall_properties object**.
3. Find **disconnect_on_idle** and these parameters:
   - **do_not_check_idleness_on_icmp_packets**
   - **do_not_check_idleness_on_these_services** - Enter the port numbers for the services that you want to ignore when idleness is checked.
   - **enable_disconnect_on_idle** - to enable the feature
   - **idle_timeout_in_minutes**
4. Save and install the policy.

### Intelligent Auto-Detect

Endpoint Security VPN use different network transports in parallel and automatically detects which is preferable. It always detects the optimal connectivity method for IKE and IPSec (and for IPSec transport during Roaming), so there is no additional configuration in the client.

Current transports in use:

- **Visitor Mode** - TCP encapsulation over port 443 (by default). This mode is used when NAT-T is not available in routing to the gateway [for example, if there is a proxy or hotspot]. Clients need Visitor Mode to operate.
Configuring Client Features

- **NAT-T** - UDP encapsulation over port 4500 (by default) and preferable transport for IPSec. The IPSec protocol does not deal with NAT devices, so Endpoint Security VPN uses NAT-T encapsulation. NAT-T packets must go back to the client through the same interface they entered from. We recommend that you put the gateway in a public DMZ with one interface for all traffic. You can also deploy the default route as the outbound route to the Internet.

**To configure auto-detect of network transports:**

1. Open GuiDBedit.
2. Open **Properties > Firewall Properties** and find the `endpoint_vpn_ipsec_transport` parameter.
3. Make sure that the `auto_detect` value is selected (default).
4. Save changes and close GuiDBedit.
5. Open SmartDashboard or SmartConsole and install the policy.

**Configuring Hotspot Access**

Endpoint Security VPN users may need to access the VPN over the Internet from a public Wireless Hotspot or Hotel Internet portal. The Desktop Policy may block hotspot access. To let all your users connect to Hotspots as needed, configure these settings for SmartDashboard-managed clients.

**To enable hotspot registration:**

1. Open **Global Properties**:
   - **Pre-R80** - In SmartDashboard, open **File > Policy > Global Properties**.
   - **R80.x** - In SmartConsole, open **Menu > Global Properties**.
2. Open **Global Properties > Remote Access > Hot Spot/Hotel Registration**.
3. Select **Enable registration**.
4. Set the **Maximum** time and add **Ports** to be used.
5. Select a **Track** option.
6. Click **OK**.
7. Save and install the policy.

**Note** - Local subnet access only and Allow access to maximum of: are not supported for this release.

**Configuring Automatic Hotspot Detection**

By default, clients automatically detect hotspots. You can change this in the TTM configuration file on the gateway.

**To change the hotspot detection setting from the configuration file:**

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the gateway. Find:

   ```
   :hotspot_detection_enabled ( 
     :gateway ( 
       :default (true) 
     )
   )
   ```

   - **true** (default) - Enables hotspot detection.
   - **false** - Disables hotspot detection.
2. Save the file.
3. Install the policy.

When clients download the new policy from the gateway, configuration changes are applied.

**Supported Algorithms and Protocols**

These algorithms are supported by Endpoint Security VPN to use with IKE:

- 3DES
- AES-128, AES-256
- MD5
- SHA-1, SHA-256
- Diffie-Hellman Group 2 (1024), Diffie-Hellman Group 14 (2048)

These transport protocols are supported by Endpoint Security VPN:

- NAT traversal with UDP encapsulation, with allocated port set to **UDP VPN1_IPSEC_encapsulation**.
- Visitor Mode through TCP connection with predefined port. By default, port 443.
Chapter 5

The Configuration File

In This Section:

- Editing the TTM File ................................................................. 38
- Centrally Managing the Configuration File ................................. 39
- Understanding the Configuration File ........................................ 39

Policy is defined on each gateway in the trac_client_1.ttm configuration file located in the $FWDIR/conf directory.

Editing the TTM File

When the client connects to the gateway, the updated policy is downloaded to the client and written in the trac.config file.

If you make changes in the trac_client_1.ttm file of a gateway, you must install the policy on each changed gateway.

Note - When you edit the configuration file, do not use a DOS editor, such as WordPad or Microsoft Word, which change the file formatting.

The TTM file must stay in UNIX format. If you do convert the file to DOS, you must convert it back to UNIX. You can use the dos2unix command, or open it in an editor that can save it in a UNIX format.

To activate changes in the TTM file:

1. Edit and save the file.
2. Install the policy in one of these ways:
   - In SmartDashboard, select Policy > Install and install Network Security on each changed gateway.
   - In R80.x SmartConsole, select Install Policy and install Access Control on each changed gateway.
   - Run cpstop and cpstart from the CLI of each changed gateway.

Important - If you use Secondary Connect or MEP, make sure that the TTM files on all gateways have the same settings.
Centrally Managing the Configuration File

If the configuration file on each gateway is identical, you can manage one copy of the configuration file on the Security Management Server. This file is copied to the gateways when you install the policy.

**Important** - You must use the newest configuration file installed on the gateway for Endpoint Security VPN. If you do not install the newest configuration file on the Security Management Server, the server will have an outdated configuration file that does not support new features.

To centrally manage the configuration file on gateways:

1. On the gateway, save a backup of `$FWDIR/conf/trac_client_1.ttm`.
2. From the gateway, copy `trac_client_1.ttm` to the server.
3. Open `$FWDIR/conf/fwrl.conf` and find the `% SEGMENT FILTERLOAD` section.
4. In the NAME section, add this line:
   ```plaintext
   NAME = conf/trac_client_1.ttm; DST = conf/trac_client_1.ttm;
   ```
   This copies the file to the Endpoint Security VPN gateways each time that you install the policy on the gateways.
5. Save the file.
6. In SmartDashboard or R80.x SmartConsole, install the policy on all gateways.

When clients download the new policy from the gateway, configuration changes are applied.

Understanding the Configuration File

The `trac_client_1.ttm` file contains sets that look like this:

```plaintext
:attribute {
  :gateway {
    :ext ()
    :map ()
    :default ()
  }
}
```

- **attribute** - The name of the attribute on the client side. This is in `trac.defaults` on the client.
- **gateway** - The name of the attribute on the gateway side. This is in `objects.c` on the Security Management Server. Look in the `objects.c` file to see what the defined behavior is on the gateway side. The name of the attribute is only written here if it is different than the name on the client side. If there is no value for `gateway`, the name of the attribute is the same in `trac.defaults` and `objects.c`.
- **ext** - If present, it is a hard coded function that is defined and done on the gateway. Do not change it. This function can be done in addition to the function defined for the attribute on the client or gateway side.
- **map** - Contains the valid values this attribute can have.
- **default** - The value here is downloaded to the client if the gateway attribute was not found in `objects.c`. If the value is `client_decide`, the value is defined on the client computer, either in the GUI or in the `trac.defaults` file on each client.
The behavior for each attribute is decided in this way:

1. If the attribute is defined for the gateway in objects.c file on the Security Management Server, that value is used.
2. If the attribute is NOT defined for a gateway in the objects.c file, the behavior for the attribute is taken from the default value.
3. If the default value is client_decide or empty, the behavior is taken from the client.
   - If the attribute is configured in the client GUI, it is taken from there.
   - If the attribute is not configured in the client GUI, it is taken from the trac.defaults file on each client.

Example:

```plaintext
:enable_password_caching {
   :gateway ()
   :default [client_decide]
}
```

enable_password_caching is the name of the attribute in trac.defaults and objects.c. Search the objects.c file on the Security Management Server to see if it is defined for the gateway.

   - If the attribute is defined for the gateway, that behavior is used.
   - If the attribute is NOT defined for a gateway, the default value is used. Because the default value is client_decide, the setting is taken from each client.

Configuration File Parameters

ред Note - Some of the parameters shown are not supported in this release. Keychain certificates are managed by the enable_capi parameter.

Collecting Logs

Each client can collect its logs into a cab file.

To collect logs on a client:

1. Click the client icon in the menu bar, and select VPN Options.
2. Open the Advanced tab.
3. Make sure Enable Logging is selected.
4. Reproduce the issue.
5. Click Collect Logs.
   This takes some time.

When the log collection is complete, a Finder window opens with the log location. Alternatively you can find the log file in /private/tmp.

Endpoint Security VPN Files

Some files in the Endpoint Security VPN installation directory can be useful in troubleshooting. Notice filenames that include trac: Total Remote Access Client. Endpoint Security VPN is a trac version.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Notes and Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security VPN.app</td>
<td>Endpoint Security VPN application GUI</td>
<td>In /Applications</td>
</tr>
<tr>
<td>cpfw.kext</td>
<td>The Firewall kernel extension bundle.</td>
<td>In /System/Library/Extensions</td>
</tr>
<tr>
<td>trac.log*</td>
<td>Logs of the client service actions.</td>
<td>Numbered files are logs saved from the log-roll. The highest number is the oldest. The trac.log file without a number is the latest.</td>
</tr>
<tr>
<td>Filename</td>
<td>Description</td>
<td>Notes and Location</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TracSrvWrapper</td>
<td>The Endpoint Security VPN daemon.</td>
<td>In /Library/Application Support/Check Point/Endpoint Connect/</td>
</tr>
<tr>
<td>desktop_policy.ini</td>
<td>The desktop policy.</td>
<td>In /Library/Application Support/Check Point/Endpoint Connect/</td>
</tr>
<tr>
<td>user_group.ini</td>
<td>Groups that the authenticated user belongs to.</td>
<td>If a user has an issue with permissions, open this file and check the groups listed. The client will restrict access if the user belongs to a group with restrictions. If a user belongs to multiple groups, the policy rules are matched in order. If group A limits permissions of group B, and rule 1 blocks traffic for group A before rule 2 allows that traffic, the user matches rule 1 and that traffic is blocked. In /Library/Application Support/Check Point/Endpoint Connect/</td>
</tr>
<tr>
<td>helpdesk.log</td>
<td>Log of basic actions of the client service.</td>
<td>Logged events include: connect, disconnect, idle, upgrade, and similar client actions. In /Library/Application Support/Check Point/Endpoint Connect/</td>
</tr>
<tr>
<td>trac_fwpktlog.log</td>
<td>Log of firewall activity with rule number.</td>
<td>Display firewall packet drop and accept logs.</td>
</tr>
<tr>
<td>collect_logs.sh</td>
<td>Collects logs.</td>
<td>If the Collect Logs action did not work (for example, if the computer was shut down before the logs finished collecting), run this script on a client to run the collection and see the verbose output of the log collections. This script expects a single parameter to reflect the resulting archive file name. In /Library/Application Support/Check Point/Endpoint Connect/</td>
</tr>
<tr>
<td>LangPack1.xml</td>
<td>Translated resource files.</td>
<td>If you want to change the language of the client GUI, you can edit this XML file. The change is applied after the client restarts. You cannot add more languages to the list of supplied translations, but you can overwrite a language that you do not need with another one. For example, under French, you can put Portuguese strings. In /Library/Application Support/Check Point/Endpoint Connect/</td>
</tr>
</tbody>
</table>
Error Messages

Unsupported Services

**Symptom**
Client shows an error message:
Firewall policy contains unsupported services.
Contact your system administrator

**Causes**
Clients do not recognize all services that are in policy rules.

**Solution**
1. Open trac.log.
3. Go up two lines and find the rule number:
   ConvertRule: rule = rule-<number>, start converting...
4. Open desktop_policy.ini and find the rule number.
5. In the svc section, find the services of the rule that are not supported.
   (For example, dcerpc services are not supported.)
6. Open SmartDashboard, find the rule in the Desktop policy, and remove the
   unsupported service.

Login option not configured

**Symptom**
Client shows an error message:
Connection failed. Login option not configured.

**Causes**
A login option was changed on the gateway and the user must select a new login
option.

**Solution**
Users click the link: Click here to configure Login Option. This takes them to the
Authentication tab of the client, where they can select a different login option.

Configuring No-Router Environments

You must configure the server in SmartDashboard or R80.x SmartConsole if there is no router
between the gateway and the Endpoint Security VPN client (for example, in a lab environment).

To configure Endpoint Security VPN to operate without a router:
1. In SmartDashboard, open the properties of the Endpoint Security VPN gateway.
2. Open IPSEC VPN >Office Mode:
3. Select the Multiple Interfaces option: Support connectivity enhancement for gateways with
   multiple external interfaces.

Traffic Dropped for Anti-spoofing

**Symptom**
Traffic is dropped.

**Scenario**
For environments in which clients connect to the VPN community from internal
interfaces (and the VPN community is behind an external interface), Anti-spoofing
must be configured differently.

**Solution**
Include the office mode network in the internal interface Anti-spoofing settings.
MEP

If you have trouble using multiple gateways with MEP, check that the Hotfix is properly installed on all gateways running a Check Point version that requires a Hotfix.