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**
For more about this release, see the E80.71 home page

**Latest Version of this Document**
Download the latest version of this document

To learn more, visit the Check Point Support Center

**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 Remote Access Clients for Windows 32/64-bit E80.71 Administration Guide.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29 Nov 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction to Remote Access Clients

In This Section:
- Endpoint Security VPN ......................................................... 8
- Check Point Mobile for Windows .............................................. 9
- SecuRemote ........................................................................ 9
- Feature Overview ................................................................... 9
- Topology Architecture .......................................................... 13

The Remote Access VPN Software Blade provides a simple and secure way for endpoints to connect remotely to corporate resources over the Internet, through a VPN tunnel. Check Point offers multiple enterprise-grade clients to fit a wide variety of organizational needs.

The clients offered in this release are:

- **SmartEndpoint-managed Endpoint Security VPN** - The Remote Access VPN blade as part of the Endpoint Security Suite lets users connect securely from their Endpoint Security-protected computer to corporate resources. The Compliance blade is managed from SmartEndpoint, and the Firewall can be managed from SmartDashboard or SmartEndpoint. Other Endpoint Security Software Blades that can be integrated include Media Encryption & Port Protection, Full Disk Encryption, Anti-Malware, and WebCheck.

- **SmartDashboard-managed clients:**
  - **Endpoint Security VPN** - 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.
  - **Check Point Mobile for Windows** - An easy to use IPsec VPN client to connect securely to corporate resources. Together with the Check Point Mobile clients for iPhone and Android, and the Check Point SSL VPN portal, this client offers a simple experience that is primarily targeted for non-managed machines.
  - **SecuRemote** - A secure, yet limited-function IPsec VPN client, primarily targeted for small organizations that require very few remote access clients.

For a detailed feature comparison, see the *Remote Access Clients E80.71 Release Notes*.

Endpoint Security VPN

- Replaces SecureClient and Endpoint Connect.
- Enterprise Grade Remote Access Client with Desktop firewall and compliance checks.
- Secure Configuration Verification (SCV) is integrated with Windows Security Center to query the status of Anti-Virus, Windows updates, and other system components.
- Integrated desktop firewall, centrally managed from Security Management Server.
- In-place upgrade from Endpoint Security VPN R75.
- In-place upgrade from Endpoint Connect R73.
- Requires the IPsec VPN Software Blade on the gateway, and an Endpoint Container license and Endpoint VPN Software Blade on the Security Management Server.
Check Point Mobile for Windows

- Enterprise Grade Remote Access Client.
- Secure Configuration Verification (SCV) is integrated with Windows Security Center to query the status of antivirus, Windows updates, and other system components.
- Requires IPsec VPN and Mobile Access Software Blades on the gateway.

SecuRemote

- Replaces the SecuRemote client.
- Basic remote access functionality.
- Unlimited number of connections for Security Gateways with the IPsec VPN blade.
- Requires an IPsec VPN Software Blade on the gateway.
- It is a free client and does not require additional licenses.

Feature Overview

The Remote Access Clients are installed on the desktop or laptop of the user and have enhanced connectivity, security, installation, and administration capabilities.

<table>
<thead>
<tr>
<th>Main Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full IPSec VPN</td>
<td>Internet Key Exchange (version 1) support for secure authentication. A Virtual Private Network (VPN) provides a secured, encrypted connection over the Internet to your organization’s network. The VPN tunnel gives remote access users the same security that LAN users have. IPSec makes the tunnel seem transparent because users can run any application or service that you do not block for the VPN. (Compare to SSL VPN, which works through web applications only.)</td>
</tr>
<tr>
<td>Location Awareness</td>
<td>Remote Access Clients intelligently detects if it is in the VPN domain (Enterprise LAN), and automatically connects or disconnects as required. If the client senses that it is in the internal network, the VPN connection is terminated. In Always-Connect mode, the VPN connection is established whenever the client exits the internal network.</td>
</tr>
<tr>
<td>Multiple Login Options</td>
<td>Multiple login options per gateway, with multi-factor authentication schemes. Supported with R80.10 and higher gateways</td>
</tr>
<tr>
<td>Proxy Detection</td>
<td>Proxy servers between the client and the gateway are automatically detected and authenticated to if necessary</td>
</tr>
<tr>
<td>Main Capability</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dead Gateway Detection</td>
<td>If the client fails to receive an encrypted packet within a specified time interval, it sends a <em>tunnel test</em> packet to the gateway. If the tunnel test packet is acknowledged, the gateway is considered active. If several consecutive tunnel test packets remain unacknowledged, the gateway is considered inactive, or dead. You can configure this feature.</td>
</tr>
<tr>
<td>Multiple Entry Point</td>
<td>Provides a gateway High Availability and Load Sharing solution for VPN connections. For Remote Access Clients, in an environment with MEP, more than one gateway protects and gives access to the same VPN domain. MEP lets the Remote Access Clients connect to the VPN from multiple gateways.</td>
</tr>
<tr>
<td>Secondary Connect</td>
<td>Gives access to multiple VPN gateways at the same time, to transparently connect users to distributed resources. Users log in once to a selected site and get transparent access to resources on different gateways.</td>
</tr>
<tr>
<td>Visitor Mode</td>
<td>If the firewall or network limits connections to ports 80 or 443, encrypted (IPSec) traffic between the client and the gateway is tunneled through a regular TCP connection.</td>
</tr>
<tr>
<td>NAT-T</td>
<td><strong>UDP Encapsulation of IPSec Traffic.</strong> Remote Access Clients can connect seamlessly through devices that do not permit native IPSec traffic (such as firewall and access points).</td>
</tr>
<tr>
<td>Hub Mode</td>
<td>Increases security. It routes all traffic through the VPN and your gateway. At the gateway, the traffic is inspected for malicious content before being passed to the client, and you can control client connectivity.</td>
</tr>
<tr>
<td>VPN Tunneling</td>
<td>Increases connectivity performance. Encrypts only traffic targeted to the VPN tunnel, and let users go more easily to sites where security is not an issue (such as public portals and search engines).</td>
</tr>
<tr>
<td>Desktop Firewall</td>
<td>Endpoint Security VPN enforces a Desktop Firewall on SmartDashboard-managed remote clients. The administrator defines the Desktop Security Policy in the form of a Rule Base. Rules can be assigned to either specific user groups or all users; this permits the definition of flexible policies.</td>
</tr>
<tr>
<td></td>
<td>SmartEndpoint-managed clients use the Endpoint Security Firewall blade.</td>
</tr>
</tbody>
</table>

Remote Access Clients for Windows 32/64-bit Administration Guide E80.71 | 10
Main Capability | Description
--- | ---
**Compliance Policy - Secure Configuration Verification (SCV)** | SCV monitors the configuration of remote computers, to confirm that the configuration complies with organization Security Policy, and the gateway blocks connectivity for computers that do not comply. It is available in Endpoint Security VPN and Check Point Mobile for Windows.
In SmartEndpoint-managed clients, you can choose to use SCV or the Endpoint Security Compliance blade.

**Secure Domain Logon (SDL)** | Establishes a VPN tunnel before a user logs in.

**Certificate enrollment, renewal, and auto Renewal** | Enrollment is the process of application for, and receipt of, a certificate from a recognized Certificate Authority (CA), in this case Check Point’s Internal CA. The system administrator creates a certificate and sends users the registration key. The client sends this key to Security Gateway, and in return receives the certificate.

### Connectivity Features in Detail
Remote Access Clients support more connectivity features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
**Automatic Connectivity Detection** | If the IPsec VPN network connection is lost, the client seamlessly reconnects without user intervention. |

**Roaming** | If the IP address of a client changes, (for example, if the client on a wireless connection physically connects to a LAN that is not part of the VPN domain), interface roaming maintains the logical connection. |

**Multiple Sites** | Remote access users can define many gateways to connect to the VPN. If you have multiple VPN gateways, users can try another gateway if the previous one is down or overloaded. |

**Dialup Support** | Endpoint Security VPN supports dial-up connections, useful where a network is not detected. |

**Hotspot Detection and Registration** | Automatically detects hotspots that prevent the client system from establishing a VPN tunnel. Opens a mini-browser to allow the user to register to the hotspot and connect to the VPN gateway. |

**Office Mode** | Lets a remote client appear to the local network as if it is using a local IP address. This is not supported on SecuRemote |

**Extended DHCP Parameters** | When using Office Mode from a DHCP server, the Remote Access Clients gateway sends data that it got from the client to the DHCP server in the correct format - Hostname, FQDN, Vendor Class, and User Class. |
### Feature
- **Machine Idleness**: Disconnects the VPN tunnel if the machine becomes inactive (because of lock or sleep) for a specified duration.
- **Keep-alive**: Send keep-alive messages from the client to the VPN gateway to maintain the VPN tunnel.
- **VPN Connectivity to VPN-1 VSX**: Terminate VPN tunnel at Check Point VSX gateways.
- **Split DNS**: Support multiple DNS servers.
- **DHCP Automatic Lease Renewal**: Automatically renew IP addresses obtained from DHCP servers.
- **Smart Card Removal Detection**: If the Smart Card is removed from the PC, the VPN tunnel is closed.

### Deployment Features
- **Automatic Client Upgrade from the Gateway**: Clients can automatically get an upgrade package when they connect to the gateway. For SmartDashboard-managed clients only.
- **Pre-configured Client Packaging**: You can create a predefined client installation package for easy provisioning.
- **Localization**: Many supported languages.

### General Features
- **Post Connect Scripts**: Run a script on client computers after a connection to the gateway is established.

### Supported Algorithms and Protocols
These algorithms are supported by Remote Access Clients 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 Remote Access Clients:
- 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.
Topology Architecture

Remote Access Clients 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.
3. Click **Set domain for Remote Access Community**.
   The VPN Domain per Remote Access Community window opens.
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>• Remote Access Clients, 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 Remote Access Clients</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>• Remote Access Clients, 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>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 Remote Access Clients</td>
<td>• Gateway of Site 1 through encrypted VPN</td>
</tr>
<tr>
<td></td>
<td>• Permitted servers (3 and 4)</td>
</tr>
<tr>
<td></td>
<td>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>
</table>
| 1 Gateway of Site 1 | • Remote Access Clients, as their VPN gateway (5)  
• External resource (4)  
• Redirects clients (5) to external resource (4) |
| 2 Remote Access Encryption Domain | Encrypted domain of gateway (1) that includes an external resource |
| 3 Servers in Encryption Domain | External resource |
| 4 External (Internet or DMZ) resource in Encryption Domain | • Server in Encryption Domain  
• Remote Access Clients if the gateway redirects |
| 5 Remote Access Clients | • Gateway of Site 1 through encrypted VPN  
• Permitted servers (3)  
• External resource (4), through gateway redirect |
Setting Up Remote Access Clients

In This Section:

Workflow for Deploying Clients ................................................................. 16
Required Gateway Settings ........................................................................... 17
Creating Installation Package with VPN Configuration Utility .................. 22
Editing an MSI Package with CLI ................................................................. 24
Distributing MSI Packages ........................................................................... 26
Automatic Upgrade from the Gateway ......................................................... 27
Endpoint Security VPN for Unattended Machines (ATMs) ......................... 29
Using DNS for Automatic Site Detection ..................................................... 31
Updating User Sites with the Update Configuration Tool ............................ 31

Workflow for Deploying Clients

Remote Access Clients require a supported gateway version. If you use Automatic MEP, the Security Management Server or Multi-Domain Server must also be supported.

See sk67820 http://supportcontent.checkpoint.com/solutions?id=sk67820 for the requirements for your environment.

The initial workflow includes:

1. Configure the Security Gateway that clients connect to.

2. Download a client package and edit the package, if necessary.

   The options available to edit client packages depend if you have SmartDashboard-managed Remote Access Clients or SmartEndpoint-managed Remote Access Clients.


   b) SmartDashboard-managed Remote Access Clients - You can use these tools to edit the client MSI:

      ▪ The VPN Configuration Utility ("Creating Installation Package with VPN Configuration Utility" on page 22).

      ▪ Client application in Administration Mode.

      ▪ CPMSI Tool with CLI. ("Editing an MSI Package with CLI" on page 24)

3. Distribute the package.

   • Through GPO or email, using the MSI file.

   • Distribute an upgrade automatically from the Security Gateway, using the TRAC.cab file. This is only for users who are upgrading from a previous version. You cannot edit the file before you distribute it.
Required Gateway Settings

You must configure one or more Security Gateways to work with Remote Access Clients. These procedures are necessary for Remote Access Clients 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 VPN Settings for R77.x Gateways

To configure the required Remote Access VPN settings on R77.x Gateways:

1. In SmartDashboard, right click the Security Gateway and select **Edit**.
   The **Check Point Gateway** window opens.
2. Enable VPN functionality: In the **General Properties** page, in the **Network Security** tab, select the **IPSec VPN** blade.
   **Note** - This enables all IPsec VPN functionality.
3. Add the gateway to the **RemoteAccess VPN** community:
   a) From the Gateway Properties tree, click **IPsec VPN**.
   b) Under **This Security Gateway Participates in the following VPN Communities**, click **Add**.
   c) In the window that opens, select **RemoteAccess**.
   d) Click **OK**.
4. Set the VPN domain for the Remote Access community:
   a) From the Gateway Properties tree, select **Topology > VPN Domain**.
   b) Click **Set domain for Remote Access Community**.
   c) In the window that opens, select the **RemoteAccess** VPN Community and click **Set**.
   d) In the window that opens, select a VPN Domain and click **OK**, or click **New** and define a VPN domain.
   e) Click **OK**.
5. Configure **Visitor Mode**:
   a) From the Gateway Properties tree, select **VPN Clients > Remote Access**.
   b) Select **Support Visitor Mode** and leave **All Interfaces** selected.
   c) Optional - Choose the Visitor Mode **Service**, which defines the protocol and port of Endpoint Security VPN connections to the gateway.
6. Configure **Office Mode**:
   a) From the Gateway Properties tree, select **Office Mode**.
   b) Select an option: **Offer Office Mode to group** or **Allow Office Mode to all users**.
   c) Select an **Office Mode Method**.
d) Click OK.

Note - Office mode is not supported in SecuRemote. If you use SecuRemote, you can select Do not offer Office Mode. If another option is selected, it is ignored.

To add Remote Access Clients users to the VPN Community:
1. In SmartDashboard, open the IPSec VPN tab.
2. In the list of VPN Communities, double click the RemoteAccess community.
3. From the tree, select Participant User Groups.
4. Make sure all Remote Access Clients client users are included.
   - You can leave All Users.
   - You can click Add to add existing user groups to the community.
   - You can click New to create a new user group or add an LDAP group.
5. Select Participating Gateways.
6. Make sure that the Security Gateway you configured for remote access is listed.
7. Click OK.

To configure encryption for the VPN:
1. From the SmartDashboard menu, select Policy > Global Properties.
   - In Support encryption algorithms - Make sure that at least one AES encryption algorithm is selected.
   - In Use encryption algorithm - Make sure that at least one AES encryption algorithm is selected.
4. Click OK.
5. Click OK.

Important - The client does not support DES algorithms. An AES algorithm must be selected.

You can enable support for DES algorithms, if you also enable support for at least one AES algorithm.

6. In the Support Data Integrity list, you can enable SHA-256 encryption in both the Phase 1 and Phase 2 tabs.

Configuring VPN Settings for R80.x Gateways

To configure the required Remote Access VPN settings on R80.x Gateways:
1. In SmartConsole > Security Policies tab, right click the Security Gateway and select Edit.
   The Check Point Gateway window opens.
2. Enable VPN functionality: In the General Properties page, in the Network Security tab, select the IPSec VPN blade.
   Note - This enables all IPsec VPN functionality.
3. Add the gateway to the **RemoteAccess VPN** community:
   a) From the Gateway Properties tree, click **IPsec VPN**.
   b) Under **This Security Gateway Participates in the following VPN Communities**, click **Add**.
   c) In the window that opens, select **RemoteAccess**.
   d) Click **OK**.

4. Set the VPN domain for the Remote Access community:
   a) From the Gateway Properties tree, select **Network Management > VPN Domain**.
   b) Click **Set domain for Remote Access Community**.
   c) In the window that opens, select the **RemoteAccess VPN Community** and click **Set**.
   d) In the window that opens, select a VPN Domain and click **OK**, or click **New** and define a VPN domain.
   e) Click **OK**.

5. Configure **Visitor Mode**:
   a) From the Gateway Properties tree, select **VPN Clients > Remote Access**.
   b) Select **Support Visitor Mode** and leave **All Interfaces** selected.
   c) Optional - Choose the Visitor Mode **Service**, which defines the protocol and port of Endpoint Security VPN connections to the gateway.

6. Configure **Office Mode**:
   a) From the Gateway Properties tree, select **Office Mode**.
   b) Select an option: **Offer Office Mode to group** or **Allow Office Mode to all users**.
   c) Select an **Office Mode Method**.
   d) Click **OK**.

   **Note** - Office mode is not supported in SecuRemote. If you use SecuRemote, you can select **Do not offer Office Mode**. If another option is selected, it is ignored.

---

To add Remote Access Clients users to the VPN Community:
1. In SmartConsole, **Security Policies** tab, under **Access Tools**, click **VPN Communities**.
2. In the list of **VPN Communities**, double click the **RemoteAccess** community.
3. From the tree, select **Participant User Groups**.
4. Make sure all Remote Access Clients client users are included.
   - You can leave **All Users**.
   - You can click the plus sign to add existing user groups to the community.
5. Select **Participating Gateways**.
6. Make sure that the Security Gateway you configured for remote access is listed.
7. Click **OK**.

---

To configure encryption for the VPN:
1. From the SmartConsole menu, select **Global Properties**.
2. Select **Remote Access > VPN - Authentication and Encryption**.
3. In **Encryption Algorithms**, click **Edit**.
• In Support encryption algorithms - Make sure that at least one AES encryption algorithm is selected.

• In Use encryption algorithm - Make sure that at least one AES encryption algorithm is selected.

4. Click OK.

5. Click OK.

⚠️ Important - The client does not support DES algorithms. An AES algorithm must be selected.

You can enable support for DES algorithms, if you also enable support for at least one AES algorithm.

**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 and the SCV checks will not be applied.

For SecuRemote, you do not need a policy server.

To define a gateway as the Policy Server:

1. In SmartDashboard (R77.x) or SmartConsole (R80.x), open the gateway that will serve as the Policy Server.


3. From the Gateway Properties tree, select Other > Legacy Authentication.

4. In the Policy Server area, from the Users list, 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.

**Excluding Local Networks from Hub Mode**

When **Exclude local networks** is enabled:

- The roaming feature is disabled. When moving to another network, the tunnel disconnects and connects again in the new network.
- If the Encryption Domain network and the local network overlap, the local network traffic is still excluded and sent to the local network in clear.

If the Office Mode IP address overlaps with the local network IP addresses, the local network traffic is not excluded.

To exclude local networks when hub mode is enabled:

1. Open trac_client_1.ttm on the gateway.
2. Add `exclude_local_networks_in_hub_mode` and set its value to one of these:
   - `true` - Local networks are excluded and users cannot change this
   - `client_decide` - Configured by end user in the Site Properties > Settings tab.
   - `false` - Feature is off.
3. Save changes.
4. Install policy on the gateway.

To exclude local networks from the client:

2. Click Site Properties > Settings tab.
3. Select **Do not route traffic for local network to the gateway**.
4. Click OK.
   - The changes is applied the next time that the user connects.

**Closing TCP Sessions**

If you configure Hub mode while remote access sessions are in progress, open sessions are not affected. You can force TCP sessions that were opened before the configuration changes to close. This makes sure that Hub Mode behavior is enforced on all connections.

To close all TCP sessions on Windows clients:

1. Open trac_client_1.ttm on the gateway.
2. In the Trac_client_1 ttm file, change these values to true:
   - `close_TCP_connections_on_VPN_connect` - true/false [default]
• **fail_VPN_connect_on_closing_TCP_Connections_failure** - true/false (default)

3. Save changes.
4. Install policy on the gateway.

### Configuring Authentication Settings for Users

Configure authentication settings for the VPN gateway in Gateway object > > **VPN Clients** > **Authentication**.

If your VPN gateway is R80.x, you can configure multiple login options for a gateway, with multiple authentication factors for each login option. Users see the different login options available and select one.

For details, see the VPN documentation for your gateway version:

- **VPN Remote Access Administration Guide** (R80.10 and higher)
- **VPN Administration Guide** (Pre- R80)

### Creating Installation Package with VPN Configuration Utility

You can use the VPN Configuration Utility to edit Remote Access Clients client packages before distribution. This tool works with:

- SmartEndpoint-managed Endpoint Security VPN
- SmartDashboard-managed Remote Access Clients

The VPN Configuration Utility gives you these options:

- Replace the **trac.config** and **trac.defaults** files that users install as part of the client MSI:
  - The **trac.config** file includes VPN Site configuration
  - The **trac.defaults** file includes the default values for configuration attributes
- Enable Secure Domain Logon
- Enable using fixed MAC addresses for Office Mode IP addresses allocation
- Choose which client type to install (SmartDashboard-managed only)
- Add SCV plugins
- Add user files to the installation file
- Create a CAB installation file

### Using the VPN Client Configuration Utility

If you use this tool to create an MSI for SmartEndpoint-managed deployments, you must distribute it with an exported package, and not with Automatic Software Deployment.
To edit an MSI client package with the VPN Client Configuration Utility:

1. Get the MSI file:
   - SmartEndpoint-managed - Export a package that includes Remote Access VPN from the SmartEndpoint.
   - SmartDashboard-managed - Download the MSI from the Support Center.

2. Run `VPNConfig.exe`.
   The VPN Client Configuration Utility opens on the General tab.

3. Click Browse to select the location of the MSI.

4. Select the options and their values to include in the MSI:
   - Secure Domain Logon - To control whether the authentication credentials sent to the Domain Controller are sent through an encrypted channel.
   - Fixed MAC - To control whether to use fixed MAC address for Office Mode IP address allocation.
   - No Office Mode - To control Office Mode support.
   - Replace trac.defaults file - This file includes the default values for configuration attributes.
   - Replace trac.config file - This file includes VPN Site configuration.

   Optional: Select Overwrite user’s configuration when upgrading. When selected, if a user has an earlier version of Remote Access Clients and installs the new MSI, the old trac.config file is overwritten by the new trac.config file.

5. If you selected to replace a trac.* file, browse to the path of the trac.* file that you want to include.

   Important - If you selected to replace the trac.config file, you have to provide the path for both trac.config and trac.defaults files.

6. Optional: Create a CAB file for Standalone VPN Client only.
   Check the box Save CAB as well (Standalone VPN Client only) to create a TRAC.cab file to use for an upgrade with SmartEndpoint-managed client.
   - Create a ver.ini file with the correct build number. Make sure the build number is higher than the build number in the current ver.ini file (located in the Endpoint Client installation directory).
   - To upgrade using a customized TRAC.cab file, users need to use it together with Upgrading with a Customized Package (on page 28).

7. Optional: Open the Edit Files tab.
   Add the desired files to the installation directory. For example, a script to use with Post Connect Script ("Configuring Post Connect Scripts" on page 71).

8. Optional: Open the Advanced tab.
   - For SmartDashboard-managed clients, select a VPN Client sub type:
     - Endpoint Security VPN - To force this VPN Client sub type.
     - Check Point Mobile for Windows - To force this VPN Client sub type.
     - SecuRemote - To force this VPN Client sub type.
     - User defined (default) - To let user select the VPN Client sub type.
   - Click Add to add SCV Plugins - To make sure that Remote Access client computer is configured in accordance with the enterprise Security Policy.

9. Click Save.
10. Select the location where the new MSI will be saved.
Editing an MSI Package with CLI

For SmartDashboard-managed clients, you can edit a client MSI with the Check Point MSI Packaging Tool utility. The tool is part of the client installation at:

C:\Program Files (x86)\CheckPoint\Endpoint Connect> cpmsi_tool.exe

Syntax

package-package-file-name>
[<-in|out|add|overwrite|overwrite|overwrite|overwrite] <filename>
[<-replace_config <true|false>] [<-sdl_enable <true|false>] [<-fixed_mac <true|false>] 
[<-client_sub_type <SecuRemote|CheckPointMobile|EndpointSecurityVpn|UserDecide>]

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-in</td>
<td>Add a file &lt;filename&gt; to the package. The file can be a filename from the list below, or &quot;all&quot; for all of them. The file must exist in same directory as the MSI file. Possible files:</td>
</tr>
<tr>
<td></td>
<td>• LangPack1.xml</td>
</tr>
<tr>
<td></td>
<td>• DisconnectedPolicy.xml</td>
</tr>
<tr>
<td></td>
<td>• trac.config</td>
</tr>
<tr>
<td>-out</td>
<td>Remove a file &lt;filename&gt; from the package. The file can be a filename from the list below, or &quot;all&quot; for all of them. The file must exist in same directory as the MSI file. Possible files:</td>
</tr>
<tr>
<td></td>
<td>• LangPack1.xml</td>
</tr>
<tr>
<td></td>
<td>• DisconnectedPolicy.xml</td>
</tr>
<tr>
<td></td>
<td>• trac.config</td>
</tr>
<tr>
<td>-add</td>
<td>Add a file &lt;filename&gt; to the package. The file can be any file. It must exist in same directory as the MSI file.</td>
</tr>
<tr>
<td>-remove</td>
<td>Remove a file &lt;filename&gt;, that you added previously, from the MSI.</td>
</tr>
<tr>
<td>-overwrite</td>
<td>Overwrite a file &lt;filename&gt; with a new version of the file. It must be a file that was added.</td>
</tr>
<tr>
<td>-copyout</td>
<td>Save a file &lt;filename&gt; as a separate file.</td>
</tr>
<tr>
<td>-add_scv_plugin</td>
<td>Add a third party SCV plugin file to the package. &lt;filename&gt; is the name of the SCV plugin. The file must exist in same directory as the MSI file.</td>
</tr>
<tr>
<td>-remove_scv_plugin</td>
<td>Remove a third party SCV plugin file from the package. &lt;filename&gt; is the name of the SCV plugin.</td>
</tr>
<tr>
<td>-overwrite_scv_plug in</td>
<td>Overwrite a third party SCV plugin file that was added to the package previously.</td>
</tr>
</tbody>
</table>
-replace_config

Previously: nk
Possible values: true or false

- true - When a user upgrades the client with this MSI, the user site list is replaced but his personal data is kept. This is done by merging the old trac.config and new trac.config files.
- false - When a user upgrades the client with this MSI, the old user trac.config file is kept and is not replaced by the new trac.config file from the installation.

-sdl_enable
Enable Secure Domain Logon (SDL)
Possible values: true or false

- true - Secure Domain Logon (SDL) is enabled for the package.
- false - Secure Domain Logon (SDL) is disabled for the package.

-fixed_mac
Possible values: true or false

- true - The client will use fixed Office mode MAC addresses.
- false - The client will not use fixed Office mode MAC addresses.

-ClientSubType
Default client type.
Possible values:

- SecuRemote
- CheckPointMobile
- EndpointSecurityVpn
- UserDecide

Note -
DisconnectedPolicy.xml is on client computers in:
- Windows Vista and higher - C:\Windows\System32\drivers
- Windows XP - C:\Windows\System32

LangPack1.xml is on client computers in the installation directory:
- 32 bit - C:\Program Files\CheckPoint\Endpoint Connect
- 64 bit - C:\Program Files (x86)\CheckPoint\Endpoint Connect

Adding Initial Firewall Policy with CLI

An initial firewall policy is the last policy installed on the computer where the MSI is generated. It is enforced until the client connects to the VPN and gets a different policy.

To add an initial firewall policy to be enforced after installation, you must add 2 files to the MSI package:

- DisconncetedPolicy.xml
- desktop_policy.ini

Note - An initial firewall is only supported in a new Remote Access Clients installation. It is not supported in upgrades from previous versions in the R75/E75 series.

To add the files required for an initial firewall:

Run: cpmsi_tool -in DisconncetedPolicy.xml -overwrite desktop_policy.ini
Installing an MSI Package with CLI

To install a Remote Access Clients MSI package with CLI, use the Microsoft Windows Installer tool, **Msiexec.exe**.

Here are some examples of how to use this tool to install the Remote Access Clients MSI package. In the examples:

- **C:\Program Files\CheckPoint\Endpoint Connect** is the path of the MSI file
- **CheckPointEndpointSecurity.msi** is the name of the MSI file

### Type of Installation | Command | Notes on Flags
--- | --- | ---
**Regular** - Use this for a non-ATM installation. All prompts show. The Cancel button does not show so that users cannot stop the installation after it starts. If necessary, a restart prompt opens when the installation completes. | **"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qb**! INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect" | qb! - Basic UI level

**Silent** - Use this for an ATM installation. User interface shows on the screen but users do not press anything. If necessary, the client automatically restarts. | **"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qb-!** INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect" | qb-! - No user interaction is required

**No User Interface** - All user interface is hidden. | **"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qn** INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect" | qn - no UI

Distributing MSI Packages

You can distribute MSI files to users in different ways:

- You can send an MSI file with GPO updates.
- You can email a URL link to the client installation file on the gateway.

Users must have administrator privileges to install the MSI.

For all installation types, make sure users have whatever is needed for authentication. 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.

Some examples of client deployment options are:

- Give each user a link to the default MSI file. Make sure that users have the gateway IP address.
- Give each user a pre-defined MSI. The user runs the MSI and can connect as soon as installation is done.
Automatic Upgrade from the Gateway

You can distribute an upgrade of the Remote Access Clients from the Security Gateway, while the user is connected to it, using the TRAC.cab file.

The installation is downloaded automatically from the gateway, and it installs automatically. This is only for users who are upgrading from a previous version. You cannot edit the file before you distribute it.

To automatically update clients to this release of Remote Access Clients or a future release, upgrade the client package on the gateway. Then all clients receive the new package when they next connect.

There are two packages: one for ATM installation and one for non-ATM installation.

Each package has these files:

- TRAC_ATM.cab or TRAC.cab
- ver.ini
- CheckPointEndpointSecurityForATM.msi (packaged in the cab file)
- CheckPointVPN.msi

Users must have administrator privileges to install an upgrade with an MSI package. Administrative privileges are not required for automatic upgrades from the gateway.

Unattended (ATM) Clients

You cannot upgrade regular Remote Access Clients and unattended (ATM) Endpoint Security VPN clients from the same gateway.

Important – If you download the Automatic Upgrade for ATM file, you get a file called TRAC_ATM.cab. You must rename it to TRAC.cab before you put it on the gateway.

Distributing the Remote Access Clients From the Gateway

Use this procedure to distribute an upgrade of the Remote Access Clients from the Security Gateway.

To distribute the Remote Access Clients from the gateway:

1. On the gateway, in the $FWDIR/conf/extender/CSHELL directory, back up the TRAC.cab and trac_ver.txt files.
3. Put the new TRAC.cab and ver.ini files in the same directory on the gateway: $FWDIR/conf/extender/CSHELL
4. On a non-Windows gateway, run: chmod 750 TRAC.cab
5. Edit the trac_ver.txt file in the directory and change the version number to the number in the new ver.ini.
6. Make sure the client upgrade mode is set:
   a) Open SmartDashboard or SmartConsole (for R80.x).
   b) Open **Global Properties > Remote Access > Endpoint Connect**.
   c) Set the **Client upgrade mode** to **Ask user** (to let user confirm upgrade) or **Always upgrade** (automatic upgrade).
   d) Click **OK**.

7. Install the policy.
   When the client connects to the gateway, the user is prompted for an automatic upgrade of the newer version.

**Configuring Upgrades**

If you put a new TRAC.cab upgrade package on the gateway to deploy to clients, configure how the upgrade will work.

- **Note** - If you select **Ask user** and the user chooses not to upgrade, the next reminder will be a week later.

To configure how to deploy changes to the client:

1. Open **Policy > Global Properties > Remote Access > Endpoint Connect**.
2. Select an option for **Client Upgrade Mode**:
   - **Do not upgrade** - The client does not upgrade even when a new TRAC.cab file is available.
   - **Ask User** - If a new TRAC.cab file is available, the client opens a notification. If the user accepts, the client is upgraded in the background. If the user does not accept, the client sends a reminder on each new connection attempt.
   - **Always upgrade** - The client upgrade is transparent to the user. When done, the client notifies the user.

**Upgrading with a Customized Package**

For E80.60 and higher Windows clients, you can create a customized MSI package and deploy it from the gateway as part of the TRAC.cab file. For example, you can include a defined trac.config file and 3rd party SCV plugins.

Users must connect successfully to the gateway at least one time without upgrading before they can upgrade with a customized package

To upgrade with a customized MSI:

1. Open trac_client_1.ttm on the gateway.
2. Add upgrade_accept_customized_packages and set its value to true.
3. Create a Microsoft CAB file that contains:
   - Your MSI file renamed TRAC.msi
   - ver.ini with the correct build number
4. Sign the CAB file with a certificate that is trusted on the target computer in these local computer certificate stores:
   - The CA certificate must be trusted in the Trusted Root Certification Authorities store
   - The Publisher certificate (used to sign the CAB file) must be trusted in the local computer’s Trusted Publishers store
5. Use the procedure in Distributing the Remote Access Clients From the Gateway [on page 27].

Endpoint Security VPN for Unattended Machines (ATMs)

Endpoint Security VPN can be installed and managed locally on unattended machines, such as ATMs. Unattended clients are managed with CLI ["Remote Access Clients Command Line" on page 122] and API and do not have a User interface. Check Point Mobile for Windows and SecuRemote do not have unattended versions.


There are different installation and upgrade files for unattended clients versus regular attended clients. They are called:
   - Remote Access Clients (for Windows) MSI file for ATM
   - Remote Access Clients (for Windows) Automatic Upgrade Package for ATM

⚠️ Important - If you download the Automatic Upgrade for ATM file, you get a file called TRAC_ATM.cab. You must rename it to TRAC.cab before you put it on the gateway.

Endpoint Security VPN clients that connect to a gateway that has an updated TRAC.cab file can be prompted to get the automatic upgrade. Because unattended clients and attended clients require different cab files, you cannot upgrade them from the same gateway.

Starting with Remote Access Clients E75.20, if an unattended client gets an automatic upgrade from the gateway, the upgrade is silent. If necessary, the client automatically restarts.

We recommend that attended clients and unattended clients connect to different gateways. If they must connect to the same gateway, do not upgrade clients automatically from the gateway. Instead, upgrade attended and unattended clients with the applicable MSI file.

Configuring the client for ATMs

ATM machines must be configured for non-interactive upgrades and continuous connectivity. ATM clients are supported on SmartDashboard-managed Endpoint Security VPN clients.

- Make sure that there is an application that uses the client API to start and monitor the connection.
  You can configure the client for always-connect (rather than the API). But we do not recommend this if you use secondary connect. If the primary tunnel disconnects and the machine reboots, a client in always-connect will not connect to the backup tunnel. It will try to connect to the primary tunnel.
  If you want always-connect and secondary connect, we recommend that you use a 3rd party code to switch to the secondary tunnel on failover.
- Make sure the ATM machine has a certificate in the CAPI, and that the client is configured for automatic CAPI re-authentication.
Administrators can configure username and password caching for ATM devices in the Windows registry. Credentials are saved encrypted in the registry per site. This feature does not depend on password caching. See Remote Access Clients Command Line (on page 122) for feature usage.

To enable the feature, a new attribute was added to the trac.defaults file: "save_cli_credentials_for_ATM" with the default value false.

To enable automatic CAPI re-authentication:
1. On the gateway, open: $FWDIR/conf/trac_client_1.ttm
2. Add these lines:
   ```plaintext
   :automatic_capi_reauthentication ( 
     :gateway (automatic_capi_reauthentication 
       :default (true) 
     )
   )
   ```
3. Save the file and install policy.
4. Apply this configuration to all gateways.

   **Note** - To learn more about the TTM file, see The Configuration File (on page 98).

Configuring the Client Package

Due to security considerations, users must approve the fingerprint and certificate DN for all primary Security Gateways in the site. Therefore, clients must connect interactively at least once for each gateway that becomes primary. With this release, a secondary gateway can become primary automatically.

To configure the package for ATMs:
1. Install non-ATM Endpoint Security VPN on a client machine.
2. Create a site.
   For each Security Gateway on the site, users have to connect and approve the fingerprint.

   **Note** - The last connected Security Gateway will be defined as the primary gateway in the generated package deployment.

3. Go to c:\program files\checkpoint\endpoint and run AdminMode.bat.
4. Go to VPN Options > Administration tab.
5. In the Input MSI Package path field, enter the pathname of CheckPointEndpointSecurityForATM.msi.
6. Select Replace user's configuration when upgrading.
7. In Select a product, select Endpoint Security VPN.
8. Click Generate.
9. Save the MSI to the local disk.
10. Enable No Office Mode on the MSI:
    a) At the Windows command prompt, go to c:\program files\checkpoint\endpoint.
    b) Run this command:
        ```plaintext
        cpmsi_tool.exe CheckPointEndpointSecurityForATM.msi -NO_OFFICE_MODE
        ```
Deploying the Client Package Manually

You can upgrade clients manually. If you do this, you do not change the client on the gateway, but you must have access to the ATM or computer.

Because this procedure does not keep the updated client package on the gateway, it is recommended for testing, not production.

To upgrade the client manually:

1. Get the MSI file:
   - ATM - CheckPointEndpointSecurityForATM.msi
   - Non-ATM - CheckPointVPN.msi
2. Run the new MSI file on the ATM or computer.

Using DNS for Automatic Site Detection

To ease first-time provisioning of clients, a site can be automatically detected during site creation. The client sends a special DNS service location query (of type SRV) to the DNS servers configured on the local network, requesting the IP address and port number of the company’s VPN gateway. The local DNS server then returns the IP address and port number of the gateway. During site creation, the name of the site automatically appears on the server page of the site wizard.

This DNS query:
- Is only performed during site creation, and not on every connection operation.
- Will only work if the client is within the corporate network so that the company’s DNS server is reachable. If the client is on a host PC outside of the company during site creation, automatic site detection fails.

To configure automatic DNS site detection:

On the DNS server, create a record with these values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>CHECKPOINT_RA_</td>
</tr>
<tr>
<td>Protocol</td>
<td>_tcp</td>
</tr>
<tr>
<td>Port number</td>
<td>443</td>
</tr>
<tr>
<td>Host offering this service</td>
<td>Name of the gateway as used in the DNS record</td>
</tr>
</tbody>
</table>

Updating User Sites with the Update Configuration Tool

If you want to give users a new site configuration without giving them a whole new package, you can use the Update Configuration tool. This tool replaces user’s site configurations found in the trac.config file with a new trac.config file that you give them. It maintains user data from the old file and transfers it to the new configuration file.

The Update Configuration tool is part of the installation package (update_config_tool.exe) and therefore it can run on users’ machines to make changes to their site configurations. You must supply them with the updated trac.config file and a way for them to install it that
replaces their old trac.config file. For example, give users a script that they can run easily that will replace the old file with the new file.

⚠️ **Important** - The client version in the Administrator's computer must be the same as the version on the user's computer.

The workflow necessary to use the Update Configuration tool has two steps.

1. The administrator creates an updated trac.config file on his or her computer.
2. The administrator gives users the updated trac.config file and a way for them to easily install it on their computers, for example, a script. The script, or other method that you use, must do the steps described in Step 2: **Replace the trac.config file on a client machine** (*Using the Update Configuration Tool* on page 32).

If a user has sites that are not in the new configuration, those sites are deleted.

You can use the same trac.config file for Endpoint Security VPN, Check Point Mobile for Windows, and SecuRemote.

**Usage for Update Configuration Tool**

**Syntax**

```
update_config_tool.exe <"old trac.config file name and path"> <"product directory">
```

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>old trac.config file name and path</td>
<td>The path on the user's machine to the temporary location where they put the old trac.config file. For example, &quot;C:\Windows\Temp\trac.config&quot;.</td>
</tr>
<tr>
<td>product directory</td>
<td>The installation directory of the Remote Access Client on the user's machine. For example, &quot;C:\Program Files\CheckPoint\Endpoint Connect&quot;.</td>
</tr>
</tbody>
</table>

**Using the Update Configuration Tool**

**Step 1: Make the updated trac.config file on the administrator machine:**

1. On the administrator Remote Access client machine, add and delete sites and make changes to the configuration of your sites.
2. Copy the trac.config file from the installation directory (for example, C:\Program Files\CheckPoint\Endpoint Connect\) and save it in a temporary location, for example, your desktop. Keep the name of the file as trac.config.
3. Distribute the trac.config file to users with the instructions below.

**Step 2: Replace the trac.config file on a user machine:**

1. Stop Remote Access Clients services from the CLI:
   
   ```
   net stop tracsrvwrapper
   ```
2. Copy trac.config from the current installation directory (for example, C:\Program Files\CheckPoint\Endpoint Connect\) to a temporary directory (for example, C:\windows\temp).

3. Copy the new trac.config file (created in Step 1) to the installation directory (for example, C:\Program Files\CheckPoint\Endpoint Connect\).

4. Run the update_config tool command to transfer user information from the old file to the new file. For example:
   update_config_tool "C:\Windows\Temp\trac.config" "C:\Program Files\CheckPoint\Endpoint Connect\"

5. Start Remote Access Clients services from the CLI:
   net start tracsrvwrapper
Helping Your Users

In This Section:

<table>
<thead>
<tr>
<th>Simple Installation</th>
<th>Remote Access Clients Client Icon</th>
<th>Helping Users Create a Site</th>
<th>Changing the Login Option Settings</th>
<th>Helping Users with Basic Client Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>.................................................................</td>
<td>...............................................</td>
<td>....................................</td>
<td>................................................</td>
<td>................................................</td>
</tr>
</tbody>
</table>

This chapter is a summary of basic actions that end-users do when they install and use Remote Access Clients.

Simple Installation

For SmartDashboard-managed clients, users can easily install the client on any supported Windows computer without a reboot after installation.

To install Remote Access Clients, users do this:

1. Download the MSI package and execute it with a double-click.
2. Click Next to start.
3. Accept the agreement.
4. Select which product to install (if you did not select this in the prepackaging).
5. Confirm a destination folder.
6. Confirm that the installation should start.
7. Click Finish.

When installation is complete, the Remote Access Clients icon appears in the notification area (system tray).

For SmartEndpoint-managed client installation, see Deploying Endpoint Security Clients in the Endpoint Security Administration Guide.

Remote Access Clients Client Icon

The client icon shows the status of the client.

SmartDashboard-managed:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Disconnected" /></td>
<td>Disconnected</td>
</tr>
<tr>
<td><img src="image" alt="Connecting" /></td>
<td>Connecting</td>
</tr>
<tr>
<td><img src="image" alt="Connected" /></td>
<td>Connected</td>
</tr>
</tbody>
</table>
Helping Your Users

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Encryption (encrypted data is being sent or received on the VPN)</td>
</tr>
<tr>
<td></td>
<td>There is an issue that requires users to take action.</td>
</tr>
</tbody>
</table>

SmartEndpoint managed:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Disconnected</td>
</tr>
<tr>
<td></td>
<td>Connecting</td>
</tr>
<tr>
<td></td>
<td>Connected</td>
</tr>
<tr>
<td></td>
<td>Connected but idle</td>
</tr>
<tr>
<td></td>
<td>There is an issue that requires users to take action.</td>
</tr>
</tbody>
</table>

Helping Users Create a Site

Each client must have at least one site defined. The site is the VPN gateway. If you did not pre-configure the client for a default site, make sure your users have:

- The gateway fingerprint.
- The gateway IP address or domain name.
- The authentication method or methods 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 might 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 Remote Access Clients 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.
3. The wizard shows the progress while the Client resolves the site name or address to the actual gateway. A message shows:
   - *This may take several minutes, depending on the speed of your network connection.*
4. 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 in the Windows registry and the security warning is not opened again for the site, even if the client is upgraded.
5. The wizard shows the authentication method window or **Login Option Selection** window.
   - The options shown here depend on the method or methods configured for the gateway. If multiple login options are configured for a gateway, users can select from multiple options.
6. The user selects an option and clicks **Next**.
7. If additional authentication factors are required, more windows open until the required authentication criteria are satisfied.
   - For example:
     - If **Certificate**, the user selects **PKCS#12** or **CAPI** (make sure the user knows which to select), and clicks **Next**.
     - If **SecurID**, the user selects the type, and clicks **Next**.
     - If **Secure Authentication API (SAA)**, the user selects that and a new page opens to select the type of SAA and the DLL file. If a DLL file is already configured for the site, users do not have to select a file. Then click **Next**.
8. 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. Right-click the client icon and select **VPN Options**.
   The Options window opens.
2. On the **Sites** tab, click **New**.
   The Site Wizard opens.

OR
1. Right-click the client icon and select **Connect to**.
2. In the **Site** drop-down, select **New Site**.
   The Site Wizard opens.

Changing the Login Option Settings

When connecting to R80.x gateways, users can select from the different login options that the administrator configured for the gateway. A login option includes one or more authentication methods that users need to enter or confirm to log in to the client.

To select a different login option for authentication:
1. Open the **Authentication** tab of the client settings in one of these ways:
   - From the **Connect** window, click the link at the bottom of the window to **Change Login Option Settings**.
     The **Authentication** tab of the client settings opens.
   - From the desktop, right-click the client icon and select **VPN Options**.
     ▪ The **Options** window opens.
     ▪ In the **Sites** tab click **Properties**.
     ▪ Click the **Authentication** tab.
2. Select a **login option**.
   Under the login option are the factor or factors and the options available for those factors, such as a certificate type for **Certificate Authentication**.
3. If necessary, to activate a certificate, click **Import**, **Renew**, or **Enroll** and follow the on-screen instructions.
4. Click **OK**.
Helping Users with Basic Client Operations

Users can do basic client operations from the client icon.

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

To quickly connect to last active site, the user can double-click the client icon.
For other operations, the user can click the icon and select a command.

<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 Options window to set a proxy server, choose interface language, enable Secure Domain Logon, collect logs, and select an SAA DLL file. In SmartDashboard-managed only.</td>
</tr>
<tr>
<td>Shutdown Client</td>
<td>Closes the Client - In SmartDashboard-managed only. An open VPN is closed. A background service continues to run and responds to CLI commands. To stop the service: <code>net stop tracsrvwrapper</code> If you close Endpoint Security VPN and stop the service, the desktop firewall still enforces the security policy.</td>
</tr>
</tbody>
</table>

For more VPN options in SmartEndpoint-managed clients:

1. Right-click the client icon and select Display Overview.
2. Click Remote Access VPN Blade.
3. Click one of the link for more options:
   - Manage connection details - See details of your connection.
   - Manage settings - Manage sites and Advanced VPN settings.
   - Register to hotspot - Register to a hotspot to connect to the VPN from a hotspot.
Configuring Client Features

In This Section:

- Intel Smart Connect Technology ................................................................. 39
- HotSpot Registration ..................................................................................... 40
- Hotspot Registration with Default Browser ................................................... 40
- Managing Desktop Firewalls ......................................................................... 41
- Secure Domain Logon (SDL) .......................................................................... 48
- Multiple Entry Point (MEP) ............................................................................ 50
- Secondary Connect .......................................................................................... 56
- Link Selection for Remote Access Clients ..................................................... 58
- Machine Authentication .................................................................................. 58
- Global Properties for Remote Access Clients Gateways ............................... 62
- Certificate Enhancements .............................................................................. 68
- Split DNS ........................................................................................................ 69
- Configuring Log Uploads ................................................................................ 71
- Configuring Post Connect Scripts ................................................................. 71
- Office Mode IP Address Lease Duration ......................................................... 71
- No Office Mode - Secondary Tunnel Resilience ............................................. 72

Intel Smart Connect Technology

Intel Smart Connect Technology updates applications that automatically get their data from the Internet, such as Microsoft Windows and Outlook and social network programs. Intel Smart Connect technology does this by periodically waking the computer from sleep or standby mode.

The Intel® Smart Connect Technology feature is disabled by default.

To enable automatic Intel Smart Connect Technology:

1. On the gateway, open: $FWDIR/conf/trac_client_1.ttm
2. Add these lines:

```plaintext
:enable_intel_aocac (
  :gateway (enable_intel_aocac
    :default (true)
  )
)
```

3. Save the file and install policy.
HotSpot Registration

Hotspot registration temporarily allows endpoint connections from Hotspots in public places, such as airports and hotels, so that users can register with the portal. Hotspot registration is configured on the Security Management Server.

To configure any port for HotSpot registration:
1. Open `GuiDBedit` and connect to the Security Management Server.
2. On the Tables tab, open Global Properties > properties > firewall_properties > registration > ports.
3. Remove the pre-defined ports.
4. Add a new element that uses the string value: `<any_port>`.
5. Click File > Save all.
6. Connect to the server using SmartDashboard.
7. Open Global Properties > Remote Access > Hot Spot/Hotel Registration
   The Ports to be opened during registration field now shows `<any_port>`.

   **Note** - The client must also be able to register to the Hotspot (“hotspot_reg” on page 127).

Hotspot Registration with Default Browser

On E80.71 and higher clients, you can register to hotspots with the computer’s default browser instead of the client’s embedded browser.

To enable default browser launch:
1. Go to the Endpoint Connect Program folder:
   - 64-bit systems - `%programfiles(x86)%\CheckPoint\Endpoint Connect\`
   - 32-bit systems - `%programfiles%\CheckPoint\Endpoint Connect\`
   For clients that are part of the Endpoint Security suite, the end of the path is `CheckPoint\Endpoint Security\Endpoint Connect`.
2. Open `trac.defaults` in a text editor.
3. Locate the `open_default_browser_for_hotspot` parameter and change its value from `false` to `true`.
4. Save the file.
5. Open the Command Prompt as Administrator and run:
   ```
   > net stop TracSrvWrapper
   > net start TracSrvWrapper
   ```

To disable default browser launch:
1. Go to:
   - 64-bit systems - `%programfiles(x86)%\CheckPoint\Endpoint Connect\`
   - 32-bit systems - `%programfiles%\CheckPoint\Endpoint Connect\`
2. Open `trac.defaults` in a text editor.
3. Locate the `open_default_browser_for_hotspot` parameter and change its value from `true` to `false`. 
Configuring Client Features

4. Save the file.
5. Open the Command Prompt as Administrator and run:
   > net stop TracSrvWrapper
   > net start TracSrvWrapper

Managing Desktop Firewalls

The Check Point Desktop Firewall works with the SmartDashboard-managed Endpoint Security VPN client. It does not work with SecuRemote, Check Point Mobile for Windows, or SmartEndpoint-managed Endpoint Security VPN.

In This Section

The Desktop Firewall ................................................................. 41
Choose a Firewall Policy to Enforce ........................................ 42
Rules .......................................................................................... 43
Default Policy ............................................................................ 43
Configuring a Desktop Firewall Policy ...................................... 44
Operations on the Rule Base ...................................................... 45
Making a Rule for FTP ............................................................... 45
Planning Desktop Security Policy ......................................... 45
SecureClient and Endpoint Security VPN .............................. 45
Location-Based Policies ........................................................... 45
Allow/Block IPv6 Traffic .......................................................... 47
Logs and Alerts ........................................................................ 47
Wireless Hotspot/Hotel Registration ....................................... 47
Letting Users Disable the Firewall ......................................... 47

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

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

#### Choose a Firewall Policy to Enforce

In SmartDashboard-managed Endpoint Security VPN, the Firewall policy enforced is configured in the Desktop Policy tab in SmartDashboard.

In SmartEndpoint-managed Endpoint Security VPN, the Endpoint Security Firewall Policy Rules configured in SmartEndpoint are enforced by default. However, you can choose to use the Desktop Policy from SmartDashboard, if, for example, your environment had Endpoint Security VPN and then was upgraded to the complete Endpoint Security solution.

To configure which Firewall policy to enforce for SmartEndpoint-managed Endpoint Security VPN:

1. In SmartEndpoint, go to **Policy tab > Firewall Policy Rules**.
2. Select a **Firewall policy** action:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce the above Firewall policy</td>
<td>Use the Endpoint Security Firewall Policy Rules</td>
</tr>
<tr>
<td>Enforce Desktop Policy from SmartDashboard</td>
<td>Use the Desktop Policy from SmartDashboard</td>
</tr>
</tbody>
</table>

3. Install Policy.
4. Restart all computers included in the rule.
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.
Configuring a Desktop Firewall Policy

Before you begin, make sure that you enabled Policy Server on a gateway.

*Desktop Security Policy in R80.x and Higher*

To create a Desktop Security Policy with R80.x or higher Security Management:

1. In SmartConsole, Security Policies, under Access Control, right-click Policy and select Edit Policy.
2. In the Policy Types area, select Desktop Security.
3. Click OK. Desktop shows in list under Access Control.
5. In SmartDashboard, open the Desktop tab.
6. 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, you can include users for whom the rule applies.
   - In inbound rules, Desktop (Endpoint Security VPN) is the destination.
   - In outbound rules, Desktop is the source.
7. Save the changes in SmartDashboard.
8. Close SmartDashboard.
9. In SmartConsole, click Install Policy.
10. In the Install Policy window:
    a) Select Desktop Security.
    b) Select the gateways that are configured to handle Endpoint Security VPN traffic.
    c) Click Install.

*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.
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.

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.

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.

SecureClient and Endpoint Security VPN

If you have SecureClient and Endpoint Security VPN installed on the same machine, see *Troubleshooting Dual Support* in one of the E80.71 Upgrade Guides.

Location-Based Policies

Location-based policies add location awareness support for the Desktop Firewall using these policies:

- **Connected Policy** - Enforced when:
  - VPN is connected.
• VPN is disconnected and Location Awareness determines that the endpoint computer is on an internal network. The Connected Policy is not enforced “as is” but modified according to the feature’s mode (the disconnected_in_house_fw_policy_mode property).

• **Disconnected Policy** - Enforced when the VPN is not connected and Location Awareness sees that the endpoint computer is not on an internal network.

Location-Based Policies for Desktop Firewall are disabled by default. Do these procedures to enable Location-Based Policies.

**Note** - Make sure that the Location Awareness feature is enabled and is working correctly.

**Location Awareness Policy Configuration**

This release introduces two new properties in client configuration:

- disconnected_in_house_fw_policy_enabled – Defines if the feature is enabled or disabled.
  Possible values are:
  • true – enabled
  • false – disabled *(default)*

- disconnected_in_house_fw_policy_mode – Defines which policy will be enforced after Location Awareness detection.
  Possible values are:
  • encrypt_to_allow – Connected policy will be enforced, based on last connected user. Encrypt rules will be transformed to Allow rules *(default)*.
  • any_any_allow – “Any – Any – Allow” will be enforced.

To enable Location Awareness for desktop firewall:

1. On a gateway, open `$FWDIR/conf/trac_client_1.ttm`.
2. Add the disconnected_in_house_fw_policy_enabled entry to the file:

   ```
   :disconnected_in_house_fw_policy_enabled ( 
     :gateway (disconnected_in_house_fw_policy_enabled 
       :default (true) 
     ) 
   )
   ```

3. Save the file and install the policy.

To configure the location based policy:

1. On a gateway, open `$FWDIR/conf/trac_client_1.ttm`.
2. Add the disconnected_in_house_fw_policy_mode entry to the file:

   ```
   :disconnected_in_house_fw_policy_mode ( 
     :gateway (disconnected_in_house_fw_policy_mode 
       :default (encrypt_to_allow) 
     ) 
   )
   ```

3. Save the file and install the policy.

**Note** - It is highly recommended to configure default values for these properties in `trac_client_1.ttm` for all gateways.
Allow/Block IPv6 Traffic

By default, the desktop firewall allows IPv6 traffic to the client.

To block IPv6 traffic to the client:
1. On the Security Gateway, open this file for editing:
   $FWDIR/conf/trac_client_1.ttm
2. Add these lines:
   ```plaintext
   :allow_ipv6 {
       :gateway (allow_ipv6
       :default (false)
   }
   ```
3. Save and close the file.
4. Install policy.

Logs and Alerts

Desktop Security log messages are saved locally on the client system in:
- 32-bit systems - `C:\Program Files\CheckPoint\Endpoint Connect\trac_fwpktlog.log`
- 64-bit systems - `C:\Program Files(x86)\CheckPoint\Endpoint Connect\trac_fwpktlog.log`

Alerts are saved and uploaded to the Security Management Server, when Endpoint Security VPN connects. Alerts can be viewed in SmartView Tracker.

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.

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 Remote Access Clients 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 Domain Logon (SDL)

Secure Domain Logon ensures that authentication credentials sent to the Domain Controller are sent through an encrypted channel.

In this section

- Configuring SDL: .......................................................... 48
- Configuring Windows Cached Credentials: ................49
- SDL in Windows Vista and Higher: ......................... 49
- Disable or Enable SDL on Internal Network: ..........50

### Configuring SDL

To enable SDL:

- Clients must belong to the VPN domain.
- SDL is enabled on the clients.

**SDL for SmartDashboard-Managed Clients**

To create an SDL-enabled client:

1. Make a self-extracting client package.
2. In **Options > Advanced**, select **Enable Secure Domain Logon (SDL)**.
3. In the **Administration** tab, generate the client and then distribute it.

If you give users a client MSI without SDL enabled, each user must manually enable it and restart the computer.

*Note* - SDL is not supported on a site that uses a CAPI certificate.

To help users enable SDL on a client:

1. Right-click the client icon and select **VPN Options**.
2. In **Options > Advanced**, select **Enable Secure Domain Logon (SDL)**.
3. Click **OK**.
4. Restart the computer and log in.

To enable Remote Access Clients to use SDL:

1. On SmartDashboard, open the policy to be installed on Endpoint Security VPN clients: **File > Open**.
2. Open the **Desktop** tab.
3. Add inbound and outbound rules to allow the NetBIOS over TCP/IP service group:
   • Source and Destination = Domain Controller and Remote Access VPN
   • Service = NBT
   • Action = Allow
4. Install the policy.

Configuring Windows Cached Credentials

When the client successfully logs on to a domain controller, the user profile is saved in cache. This cached information is used if subsequent logons to the domain controller fail.

To configure this option in the client registry:
1. Go to HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon.
2. Make a new key CachedLogonCount, with the valid value range of 0 to 50.
   The value of the key is the number of previous logon attempts that a server will cache. A value of 0 disables logon caching. A value over 50 will only cache 50 logon attempts.

SDL in Windows Vista and Higher

There are different SDL modes for Windows Vista and higher:
• Explicit
• Implicit

Using Explicit Mode

SDL can be invoked explicitly prior to domain logon. In Explicit Mode, SDL is implemented as a Pre-Logon Access Provider (PLAP).

A PLAP is a Windows component that enables a Pre Logon Connection to the Internet. After SDL is enabled, or if Windows enables its own PLAP, a new Network Logon button is added to the logon screen.

To see available pre-logon connection methods (PLAPs), click the Network Logon button.

Note - In Windows 8, to get to PLAP button, from Network Logon screen click back to get to All Users screen.

Using Implicit Mode

Implicit mode SDL is invoked automatically when the user authenticates to the domain controller. The user does not configure the client to employ implicit mode.

The user cannot authenticate to the domain controller over a VPN, but the client can receive a Group Policy and logon scripts. The Windows operating system authenticates to the domain controller using the cache. Windows cached credentials must be enabled on the machine and the user must have at least one successful login cached.

Note - Implicit mode SDL is not invoked with smart card logon to Windows.
Disable or Enable SDL on Internal Network

By default, the client automatically disables Secure Domain Login (SDL) when the endpoint client is connected to an internal network or the VPN domain. Until the client gets a response from the location awareness feature, the decision is based on the fact that the client has an IP address in the VPN Domain.

To enable or disable SDL on the internal network or VPN Domain:

1. On the site’s gateway, open:
   `$FWDIR/conf/trac_client_1.ttm`
2. Search the file for: `ignore_sdl_in_encdomain`.
   If the property does not exist, create it.
3. Set the required value according to this table:

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>true (default)</td>
<td>The SDL window does not show when the client is inside the LAN or VPN domain.</td>
</tr>
<tr>
<td>false</td>
<td>The SDL window always shows.</td>
</tr>
</tbody>
</table>

4. Save and close.
5. Install policy on the Security Gateway.

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.

While Remote Access Clients automatically detects and uses MEP topology, it also supports Manual MEP.

>Note - For Check Point GO, the gateways providing MEP do not have to belong to the same VPN domain. The gateways are configured using the TTM file on each gateway.

Remote Access Clients automatically detects and uses MEP topology.

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.

To enable Implicit MEP, you must install the Hotfix on the Security Management Server and on each Security Gateway. For Manual MEP this is not necessary.
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.

Defining MEP Method

MEP configuration can be implicit or manual.

- **Implicit** - MEP methods and gateway identities are taken from the topology and configuration of gateways that are in fully overlapping encryption domains or that have Primary-Backup gateways.


Whichever you choose, you must set the Remote Access Clients configuration file to identify the configuration.

To define MEP topology:

1. On the gateway, open the `$FWDIR/conf/trac_client_1.ttm` configuration file.
2. Find `automatic_mep_topology`. If you do not see this parameter, add it manually as shown here:

   ```
   :automatic_mep_topology ( 
   :gateway ( 
   :map ( 
   :true (true) 
   :false (false) 
   :client_decide (client_decide) 
   ) 
   :default (true) 
   ) 
   )
   ```
3. Set the value of `default` to:
   - `true` - For implicit configuration
   - `false` - For manual configuration

4. **For Manual MEP only:** Make sure that `enable_gw_resolving` is `true`

5. Save the file.

6. Install the policy.

**Implicit MEP**

With Implicit MEP, the configurations of the gateways are used to make the VPN connections. Gateways are configured differently for each MEP method.

Before you begin, make sure that `$FWDIR/conf/trac_client_1.ttm` on each gateway has:

```
automatic_mep_topology (true)
```

**Configuring Implicit First to Respond**

When more than one gateway leads to the same (overlapping) VPN domain, they are in a MEP configuration. The first gateway to respond is chosen. To configure first to respond, define the part of the network that is shared by all the gateways as a single group and assign that group as the VPN domain.

Before you begin, make sure that Load Distribution is **not** selected in SmartDashboard > Global Properties > Remote Access > VPN Advanced.

To configure First to Respond MEP:

1. Find out which gateways are in the VPN domain. In the VPN CLI, run:
   
   `vpn overlap_encdom`

2. Create a host group and assign all of these gateways to it.

3. In the Properties window of each gateway network object > Topology page > VPN Domain section, select **Manually defined** and then select the host group of MEP gateways.

4. Click **OK**.

5. Install the policy.

When you work with first to respond, you can give preference to the gateway that you selected to connect to. To do this, configure a grace period. The Remote Access Client waits the length of the grace period for a response from the selected gateway. If the selected gateway does not respond within the configured time, the first gateway that responded gets the connection.

Configure the same grace period on each gateway.

**To give preference to the selected gateway:**

1. On each gateway, open the `$FWDIR/conf/trac_client_1.ttm` configuration file.

2. Find the `mep_prefer_chosen_gw_grace_period` parameter.

3. Set the grace period in milliseconds.

4. Save the file.

5. Install the policy.
Configuring Implicit Load Distribution

To configure implicit MEP for random gateway selection:

1. Open **Global Properties**.
2. Open **IPSec VPN > Advanced** (or **VPN > Advanced**).
3. Select **Enable load distribution for Multiple Entry Point configurations (Site to Site connections)**.
4. Define the same VPN domain for all the gateways:
   a) Create a group of the gateways.
   b) On the **Properties** window of each gateway network object > **Topology > VPN Domain** section, select **Manually defined**.
   c) Select the group.
5. Click **OK**.
6. Install the policy.

Configuring Implicit Primary-Backup

Configure the VPN Domain that includes the Primary gateway and another domain that includes only the backup gateway. Configure each gateway as either the Primary gateway or a backup gateway.

To configure the primary gateway:

1. Open **Global Properties** window > **VPN > Advanced**, select **Enable Backup Gateway**.
2. In the Object Explorer, click **New > Network Group** and create a group of gateways to act as backup gateways.
3. Edit the Primary gateway object and open the **IPsec VPN** page.
4. Select **Use Backup Gateways**, and select the group of backup gateways.
   This gateway is the primary gateway for this VPN domain.
5. For each backup gateway, make a VPN domain that does not include IP addresses that are in the Primary VPN domain or the other backup domains.
   If the backup gateway already has a VPN domain, you must make sure that its IP addresses do not overlap with the other VPN domains.
   a) Create a group of IP addresses not in the other domains, or a group that consists of only the backup gateway.
   b) In the backup network object, go to the **Network Management > VPN Domain** section, select **Manually defined**.
   c) Select the group.
6. Click **OK**.
7. Install the policy.
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 Remote Access Clients, 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 ["Configuring Geo-Cluster DNS Name Resolution" on page 55].

   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.

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

To enable Geo-Cluster DNS Name Resolution:
2. Change the :default attribute, located in the :enable_gw_resolving attribute, to true.
3. Manually add the mep_mode attribute and set it to dns_based.
4. Make sure that the automatic_mep_topology is false.
5. Save the file.
6. Install the policy.

To disable Geo-Cluster DNS Name Resolution (and enabling DNS IP address cache):
2. Do one of these:
   • Set the automatic_mep_topology to true
   • Set the mep_mode attribute to one of the options that is not “dns_based.” See Manual MEP (on page 54).
   • Disable the MEP entirely by setting the enable_gw_resolving attribute to false.
3. Save the file.
4. Install the policy.
Secondary Connect

Secondary Connect gives access to multiple VPN gateways at the same time, to transparently connect users to distributed resources. Users log in once to a selected site and get transparent access to resources on different gateways. Tunnels are created dynamically as needed, based on the destination of the traffic.

For example: Your organization has Remote Access gateways in New York and Japan. You log in to a VPN site that connects you to the New York gateway. When you try to access a resource that is behind the Japan gateway, a VPN tunnel is created and you can access the resource behind the Japan gateway.

Traffic flows directly from the user to the gateway, without site-to-site communication. VPN tunnels and routing parameters are automatically taken from the network topology and destination server IP address.

In an environment with Secondary Connect, the gateway that the client first authenticates to is the Primary gateway. A gateway that the client connects to through a secondary VPN, is a Secondary gateway.

For gateway requirements for Secondary Connect, see sk65312 http://supportcontent.checkpoint.com/solutions?id=sk65312.

Configuring Secondary Connect

Users can access all gateways that are in the Remote Access Community on the same Management server.

Make sure to do the configuration procedure on each Primary and Secondary gateway.

All gateways that participate in Secondary Connect must have a server certificate that is signed by the internal Certificate Authority.

If you use Office Mode IP addresses, make sure that the IP addresses are different on each gateway so there are no conflicts. The Office Mode IP address that is issued by the first gateway is used to access the secondary gateways.

If user authentication credentials are not cached, users must enter their credentials again when they try to access resources on a different gateway.

To configure Secondary Connect on each gateway:

1. Make sure the gateway has a server certificate that is signed by the internal Certificate Authority.
2. On each gateway, open the $FWDIR/conf/trac_client_1.ttm configuration file.
3. Set the :default value of automatic_mep_topology to true.
4. Find `enable_secondary_connect`. If you do not see this parameter, add it manually as shown here:

```plaintext
:enable_secondary_connect (
   :gateway (
      :map (n
         :true (true)
         :false (false)
         :client_decide (client_decide)
      )
      :default (true)
   )
)
```

5. Make sure the `:default` value of `enable_secondary_connect` is `true`.
6. Save the file.
7. Install the policy.

**Secondary Connect for Users**

When users log in to the VPN, they can select a site and gateway.

If their credentials are not cached, they might be prompted to authenticate again for a secondary connection.
Link Selection for Remote Access Clients

In This Section:
Overview .......................................................................................................................... 58
Configuring Link Selection for Remote Access .......................................................... 58

Overview
Link Selection is a method for remote peers to determine the IP address of the local gateway.

Configuring Link Selection for Remote Access

To configure Link Selection for Remote Access:
1. In SmartDashboard or SmartConsole, open Check Point Gateway properties for the gateway object.
2. Go to the IPSec VPN > Link Selection page.
3. Select the Link Selection method:
   - **Always use this IP address** - when a VPN peer tries to determine the IP address of the gateway, it always uses the IP address specified here.
   - **Calculate IP based on network topology** - when a VPN peer tries to determine the IP address of the gateway, the gateway sends the list of its internal interfaces and the networks behind them to the client. The client checks if the IP address of one of its interfaces is on a network on this list. If a match exists, it establishes a connection with the matching IP address. Otherwise, it uses the IP address of the first external interface on the gateway.

   Note - The Use DNS resolving and the Use probing methods are not available for the remote access clients.

4. Save the changes.
5. Install Policy.

Machine Authentication
Machine Authentication is a new authentication capability for the VPN client: Authentication with a machine certificate from the Windows system store.
Machine authentication supports these modes:

- **User and machine authentication** - Authenticate with a machine certificate and the selected user authentication method.
- **Machine-only authentication** - Authenticate using only a machine certificate. This mode is available before and after a user logs in to Windows.

Machine authentication is supported for these Remote Access clients:

- Remote Access client Endpoint Security VPN
- Remote Access Check Point Mobile for Windows
- Endpoint Security full suite with the Remote Access blade.

Machine authentication is not supported for Remote Access SecuRemote.

### Machine Authentication Configuration on the Gateway

To configure Machine Authentication you must have a Security Gateway version that supports that feature. For the supported Security Gateway versions and the instructions for configuring Machine Authentication, see sk121173 [http://supportcontent.checkpoint.com/solutions?id=sk121173](http://supportcontent.checkpoint.com/solutions?id=sk121173).

### Configuring the LDAP Server

Machine Authentication works with an LDAP server that is defined in SmartDashboard and added as a Trusted CA.

To add an LDAP Server object as a trusted CA:

Go to the **Servers and OPSEC** tab, right click on **Servers** and select **Trusted CAs > New CA > Trusted**.

### Configuring Machine Authentication on the Client

Configure machine authentication using the `trac.defaults` configuration file.

These attributes are available in E80.71 and higher clients:

- **enable_machine_auth** - Enables machine authentication with a machine certificate from the Windows System Store (if the certificate exists). If this parameter is set to true, authentication passes for both factors: machine certificate authentication and user authentication. If this parameter is set to false, authentication passes only with user authentication (legacy mode).
  
  Default value: true.

- **machine_tunnel_site** - Contains the display name of the site that the client will connect to, using only machine authentication.

  Default value: empty.

  **Note** - Create the machine site before configuring the default site value.

- **machine_tunnel_before_logon** - Lets the client establish a VPN tunnel before the user logs in to Windows. If this attribute is set to true and the `machine_tunnel_site` has a value, and the value matches the display name of the created site, then authentication passes only with machine certificate before the user logs in to Windows.

  Default value: true.
• **machine_tunnel_after_logon** – Lets the client ignore user authentication and authenticate using machine certificate only after a user logs in to Windows. If this attribute is set to true and the `machine_tunnel_site` has a value, and the value matches the display name of the created site, then authentication passes only with machine certificate after the user logs in to Windows.
Default value: false.

**To edit the attributes:**

1. On the client computer, open the configuration file in a text editor, with Administrator permissions.
   - **EPS** (managed client)  
     C:\Program Files (x86)\CheckPoint\Endpoint Security\Endpoint Connect\trac.defaults
   - **EPC** (standalone client)  
     C:\Program Files (x86)\CheckPoint\Endpoint Connect\trac.defaults
2. Edit the file, save, and close it.
3. Reboot the client computer.

**Configuration Examples for Machine and User Authentication**

These examples show how to configure machine and user authentication using the `trac.defaults` file on the client.

**Configuring machine and user authentication:**

Establish a user and machine tunnel after a user logs in to Windows:

1. Create a site and choose the user authentication method.
2. Set `enable_machine_auth` to true.

**Configuring machine authentication before Windows Login, and user and machine authentication after:**

This procedure explains how to configure:

- Machine authentication before a user logs in to Windows.
- User and machine authentication after a user logs in to Windows.

A machine tunnel is established automatically when the machine starts and a machine certificate is used for authentication. After a user logs in to Windows, the machine tunnel is disconnected. If `always_connect` is enabled, a user and machine tunnel is established. This tunnel is established to the last site to which the user connected from Windows. When a user logs off from Windows, the user and machine tunnel is disconnected and a machine tunnel is established.

1. Set `enable_machine_auth` to true.
2. Set `machine_tunnel_before_logon` to true.
3. Set `machine_tunnel_after_logon` to false.
4. Create the default site for the tunnel. (If this site is already defined, skip this step.)
5. Set the authentication method for the user (will be used after the Windows logon).
6. Set `machine_tunnel_site` to the display name of the default site.
Configuring Machine tunnel authentication ('Terminal' mode):
A VPN tunnel is established automatically before the user logs in to Windows. The tunnel is maintained after the user logs in to Windows and after the user logs out of Windows.

1. Define a site and choose the user authentication method.
2. Set `enable_machine_auth` to true.
3. Set `machine_tunnel_before_logon` to true.
4. Set `machine_tunnel_after_logon` to true.
5. Create the default site for the tunnel. (If this site is already defined, skip this step.)
   It is not necessary to configure the authentication method. The default setting can be used.
6. Set `machine_tunnel_site` to the display name of the default site

Notes for machine tunnel authentication:

- It is important to create the machine site before you configure the default site in the configuration file.
- In the Security Gateway object, in the VPN Clients > Authentication page, configure the authentication method as Defined on user record (Legacy authentication).
- The only way to disconnect the Machine only tunnel is to run the command `trac disconnect` from the CMD window. To prevent users from disrupting the Machine tunnel, some actions from the GUI are not permitted, for example: create site and connection buttons.
- Best Practice - Enable Always Connect when working with a Machine only tunnel.
   To enable Always Connect:
   a) Open the VPN Client.
   b) Go to VPN Options > Sites
   c) Select a default site for machine only connection.
   d) Click Properties > Settings.
   e) Select Enable Always Connect.

Creating a Customized MSI file that Supports Machine Authentication
When using machine tunnel before Windows login, or a machine tunnel before and after Windows login, we recommend using the VPN Client Configuration Utility to create a customized MSI package that supports Machine tunnel authentication.

To create a customized MSI for machine tunnel before and after Windows login:

1. Install the Endpoint Client from the MSI you want to repackage (Release E80.71 and higher).
2. Create a site, but do not connect to it. When asked for authentication method, keep the default value.
3. Edit the `trac.defaults` file and configure the machine tunnel.
4. To make sure that the client connects with a machine tunnel, restart the machine.
5. Copy the `trac.defaults` file and the `trac.config` file from the installation directory to a different directory.
6. Open the VPN Client Configuration Tool ("Creating Installation Package with VPN Configuration Utility" on page 22):
   a) Choose the MSI you want to repackage.
   b) Select the Replace trac.defaults file and the Replace trac.config file.
   c) In the Advanced tab, select the VPN client sub type. To ask the user during the installation which flavor to install, leave it as User defined (default)

To upgrade from a Gateway with the customized MSI:
Upgrading with a Customized Package (on page 28)

Global Properties for Remote Access Clients Gateways

Many Remote Access Clients properties are centrally managed on the server, rather than per gateway or per client.

To configure Remote Access Clients features in Global Properties:
1. Open Global Properties:
   - Pre-R80 - In SmartDashboard, open File > Policy > Global Properties.
   - R80.x - In SmartConsole, open Menu > Global Properties.
2. Open Remote Access > Endpoint Connect.
4. Set Connectivity Settings:
   - Connect Mode (on page 63)
   - Location Aware Connectivity (on page 64)
   - Disconnect when connectivity to network is lost ("Roaming" on page 63)
   - Disconnect when device is idle ("Idle VPN Tunnel" on page 66)
5. Set Security Settings.
7. Click OK.
8. Install 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 **Connect Mode** 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** - Remote Access Clients will automatically establish a connection to the last connected gateway.

- **Configured on endpoint client** - Connection method is set by each Remote Access Clients client. In the client, this is configured on **Sites > Properties > Settings**.

### Roaming

If the main IP address of a client changes, interface roaming maintains the logical connection. The client tries to reconnect on every interface change. It stays in *Reconnecting* status until the network connection is returned or roaming times out.

**Disconnect when connectivity to network is lost:**

- **No** - Roaming is set with unlimited timeout. The client keeps trying to reconnect until the session times-out.

- **Configured on the endpoint client** - Default client configuration sets this option to false, so roaming is unlimited by default. If you create a client MSI that enabled the Disconnect option for clients, roaming is limited to the set time-out (default is 2 minutes).

- **Yes** - Roaming is limited by a time-out that is 2 minutes by default. The client will give up on Roaming after the time-out passes and will fail the connection. If the time-out is set to 0, the client does not try to reconnect automatically after the main IP address changes.

You can configure how long the client will continue to roam until it fails the connection.

**To configure the roaming timeout:**

1. Open GuiDBedit.
2. Open the **Global Properties** category and find the `endpoint_vpn_implicit_disconnect_timeout` parameter.
3. Enter the number of minutes that you want clients to roam before failing the connection.

   **Note** - Some gateways do not accept a zero value for this setting.

4. Save the changes.
5. Close GuiDBedit.
6. Open SmartDashboard or SmartConsole and install the policy.

Location Aware Connectivity

Remote Access Clients intelligently detects whether or not it is inside the VPN domain (Enterprise LAN), and automatically connects or disconnects as required.

When the client is detected within the internal network, the VPN connection is terminated.

If the client is in **Always-Connect** mode, the VPN connection is established again when the client exits.

Choose a location awareness configuration.

- **Interface-topology-based** (recommended)
  The location is determined by the gateway interface that received the client connection. If the client connection came from an external interface of the gateway, the client’s location is considered to be in the external network. If the client connection came from an internal interface of the gateway, the client’s location is considered to be in the internal network. For an interface listed as both external and internal, the location is considered external.

- **Specific network considered as internal**
  The originating IP of the client connection, as seen from the gateway, is compared to a configured list of internal networks. To use this setting, you must configure the internal networks.

- **Domain Controller (DC) connectivity** (default but limited)
  The location is based on the availability of the DC on the client network, assuming the DC is accessible only from within the internal network (not externally or through the VPN tunnel).

Enabling Location Awareness

To enable location awareness:

1. In SmartDashboard or R80.x SmartConsole, open **Global Properties** > **Remote Access** > **Endpoint Connect**.
2. In **Location Aware Connectivity or Network Location Awareness** select **Yes**.
3. Click **Configure**.

Configuring Location Awareness in pre-R75 Gateways

After you enable the Location Aware Connectivity feature, configure how it will operate.

To configure location awareness for topology in gateways before R75:

1. After enabling the Location Awareness feature, save the policy and close SmartDashboard.
3. On the **Tables** tab, open **Global Properties > Properties > firewall_properties**.
4. Open **endpoint_vpn_preferences > endpoint_vpn_la_preferences** and find the **la_use_gw_topology_to_identify_location** property.
5. Set the **Value** field in the **Edit** textbox to **True**.
6. Save and close.
7. Open SmartDashboard.
Configuring Client Features

8. Install the policy.

To configure location awareness based on internal networks or the domain Controller in gateways before R75:

1. In Global Properties > Endpoint Connect, click Configure by Location Aware Connectivity. The Location Awareness Settings window opens.

2. Select how clients are identified as internal.
   a) **Client can access its defined domain controller.** Checks if the client can access the Microsoft Domain controllers on the internal network, which are inaccessible through a VPN tunnel.
   b) **Client connection arrives from the following networks.** Define a group of known internal networks. Click Manage to define a network.

   Note - If the client is behind a NAT device, include the NAT Device IP address in the internal network.

3. Click OK.
4. Install the policy.

*Configuring Location Awareness in R75 and Higher Gateways*

To configure Location Awareness in R75 and higher gateways:

1. In SmartDashboard or R80.x SmartConsole, open Global Properties > Remote Access > Endpoint Connect.

2. In Connectivity Settings, in Network Location Awareness, select Yes and click Configure. The Network Location Awareness window opens.

3. Select a location awareness configuration.
   - **The client connects to the gateway through one of its internal interfaces** - This option, based on interface topology, is recommended and selected by default.
   - **The client connects from this network or group** - Select this to specify the network considered to be internal.
   - **The client runs on a computer that can access its Active Directory Domain** - Bases the location on the availability of the Active Directory Domain Controller.

4. Click OK.

*Optimizing External Network Detection*

To set fast detection, in the Location Awareness Settings window, click Advanced. The Location Awareness - Fast Detection of External Locations window opens.

These settings are optional. Their only purpose is to identify external networks quickly (queried locally before contacting a remote service).

- **Regard wireless networks as external.** Wireless networks you define here are internal. Of the client’s wireless IP address is from one of these networks, it is considered internal. All other wireless networks are considered external.
• **Consider DNS suffixes which do not appear in the following list as external.** Define DNS suffixes that Remote Access Clients identifies as internal. If you select this option, make sure to define all internal DNS suffixes.

• **Remember previously detected external networks.** Networks previously identified by the client as external can be cached (on the client side), so future encounters with them result in immediate detection.

Selecting one or more of these options enhances the performance of location awareness.

The location detection mechanism will go through the different settings and stop once a match to “external” is found; otherwise it will move on to the next setting, until eventually it reaches either of the last two decisive tests (RAS or DC), the only reliable tests on the basis of which to conclude “inside.”

---

### 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

Remote Access Clients 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.

- **NAT-T** - UDP encapsulation over port 4500 (by default) and preferable transport for IPSec. The IPSec protocol does not deal with NAT devices, so Remote Access Clients 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.

### Smart Card Removal Detection

We recommend that you configure Remote Access Clients to disconnect a user session when the user removes the smart card from the reader, or disconnects the card reader from its USB port. The system shows the message:

VPN tunnel has disconnected. Smart card was removed.

**To enable Smart Card removal detection:**

1. On the gateway, open `$FWDIR/conf/trac_client_1.ttm`.
2. Locate the `disconnect_on_smartcard_removal` line.

```plaintext
:disconnect_on_smartcard_removal ( 
    :gateway ( 
        :default (true) 
    ) 
)
```

3. Change the `:default` property as follows:
   - **true** - Enables smart card removal detection for all connections to the current gateway.
   - **false** - Disables smart card removal detection for all connections to the current gateway.
   - **client_decide** - Enables or disables smart card removal detection individually for each client.
4. Save the file and install the policy.

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

### Configuring Hotspot Access

Remote Access Clients 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**

You can configure the clients to automatically detect hotspots and open an embedded browser for quick registration.

To enable hotspot registration from the configuration file:

1. Edit the $FWDIR/conf/trac_client_1.ttm file on the Security Gateway.

   ```ttm
   :hotspot_detection_enabled (  
     :gateway (   
       :default (true)   
     )  
   )
   :hotspot_registration_enabled (  
     :gateway (   
       :default (false)   
     )  
   )
   ```

2. Change these parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hotspot_detection_enabled</td>
<td>true</td>
<td>Set to True to enable hotspot detection.</td>
</tr>
<tr>
<td>hotspot_registration_enabled</td>
<td>false</td>
<td>Set to True to enable a user to get a hotspot registration page (in embedded browser).</td>
</tr>
</tbody>
</table>

3. Save the file.

4. Install the policy on this Security Gateway.

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

**Certificate Enhancements**

On E80.60 and higher Windows clients you can:

- Display the Friendly Name for a certificate
- Filter certificates according to the Enhanced Key Usage attribute (certificates without client authentication are not shown)
- Choose not to show expired certificates in the certificate selection list

Configure these features in the `trac_client_1 ttm` configuration file.
To configure the new functionality:

In the trac_client_1 ttm configuration file, configure these parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>display_capi_friendly_name</td>
<td>Valid values: 0 and 1 (default). Make sure it is set to 1 to show the Friendly Name.</td>
</tr>
<tr>
<td>display_expired_certificates</td>
<td>Valid values: 0 (default) and 1. Make sure it is set to 0 to not show expired certificates in the certificate selection list.</td>
</tr>
<tr>
<td>display_client_auth_certificates_only</td>
<td>Valid values: 0 and 1 (default). Make sure it is set to 1 to only show certificates that have Client Authentication as part of their extended key usage.</td>
</tr>
</tbody>
</table>

Note - Only ASCII characters are supported in Friendly Names.

Split DNS

The client must use an internal DNS server to resolve the names of internal hosts (behind the Security Gateway) with non-unique IP addresses. For Endpoint Security VPN and Check Point Mobile for Windows, you can do this with Office mode. In SecuRemote, you can do this with the split DNS feature.

Split DNS uses a SecuRemote DNS Server, an object that represents an internal DNS server that you can configure to resolve internal names with unregistered, (RFC 1981-style) IP addresses. It is best to encrypt the DNS resolution of these internal names.

After you configure a SecuRemote DNS server to resolve traffic from a specified domain and install policy, it takes effect. If users try to access that domain while connected to the VPN, the request is resolved by the SecuRemote DNS server. The internal DNS server can only work when users are connected to the VPN.

You can configure multiple SecuRemote DNS servers for different domains.

Configuring Split DNS

To configure a SecuRemote DNS server for Split DNS:

1. Create a **New SecuRemote DNS**:
   - Pre-R80 - In SmartDashboard, go to the **Servers and OPSEC Applications** tab of the Objects Tree.
     Right-click **Servers** and select **New SecuRemote DNS**.
   - **R80.x** - In SmartConsole, in the Objects tree, select **New > Server > More > SecuRemote DNS**.
     The **New SecuRemote DNS** window opens.

2. In the **General** tab, enter a name for the server and select the host on which it runs.

3. In the **Domains** tab, click **Add** to add the **domains** that will be resolved by the server.
The Domain window opens,

4. Enter the **Domain Suffix** for the domain that the SecuRemote DNS server will resolve, for example, checkpoint.com.

5. In the **Domain Match Case** section, select the maximum number of labels that can be in the URL before the suffix. URLs with more labels than the maximum will not be sent to that DNS.
   - **Match only *.suffix** - Only requests with 1 label are sent to the SecuRemote DNS. For example, “www.checkpoint.com” and “whatever.checkpoint.com” but not “www.internal.checkpoint.com.”
   - **Match up to x labels preceding the suffix** - Select the maximum number of labels. For example, if you select 3, then the SecuRemote DNS Server will be used to resolve “www.checkpoint.com” and “www.internal.checkpoint.com” but not “www.internal.inside.checkpoint.com”.

6. Click **OK**.
7. Click **OK**.
8. Install the policy.

**Enabling or Disabling Split DNS**

On SecuRemote, Split DNS is automatically enabled. On Endpoint Security VPN and Check Point Mobile for Windows, you can edit a parameter in the trac_client_1.ttm configuration file to set if Split DNS is enabled, disabled, or depends on the client settings.

To change the setting for Split DNS on the gateway:

1. On the gateway, open the $FWDIR/conf/trac_client_1.ttm file with a text editor.
2. Add the **split_dns_enabled** property to the file:

   ```plaintext
   :split_dns_enabled ( 
     :gateway ( 
       :map ( 
         :true (true) 
         :false (false) 
         :client_decide (client_decide) 
       ) 
       :default (client_decide) 
     ) 
   )
   ```

3. Set the value in the **:default** attribute:
   - **true** - enabled
   - **false (default)** - disabled
   - **client_decide** - Takes the value from a file on the client machine
4. Save the file and install the policy.
Configuring Log Uploads

You can have firewall and SCV logs from SmartDashboard-managed clients sent to the Security Management Server. Logs are accumulated by each client according to the Desktop Policy, and sent when the client next connects. You can open the logs with SmartView Tracker.

To configure log uploads for Desktop Policy and SCV logs:
1. In the policy, set the rules that you want clients to log to Track = Alert.
2. On each gateway, open the $FWDIR/conf/trac_client_1.ttm configuration file.
3. Set fw_log_upload_enable to true.
   If false, the client will not accumulate logs, regardless of the rule Track settings.
4. Save the TTM file.
5. Install the policy.

Configuring Post Connect Scripts

The Post Connect feature lets you run a script on client computers after connection is established. You must make sure that the script resides on the client computers, in the correct path.

To set the script path:
1. Open GuiDBedit.
2. Set desktop_post_connect_script to a full path on client machines for a script that Remote Access Clients will run after a connection is established (leave empty to disable the feature).
3. Set desktop_post_connect_script_show_window to true to make the script run in a new window. (The default is false. The script runs in a hidden window.).
4. Save and close GuiDBedit.
5. Install the policy.

Office Mode IP Address Lease Duration

When a remote user’s machine is assigned an Office mode IP address, that machine can use it for a certain amount of time. This time period is called the “IP address lease duration.” The remote client automatically asks for a lease renewal after half of the IP lease duration period has elapsed. If the IP lease duration time is set to 60 minutes, a renewal request is sent after 30 minutes. If a renewal is given, the client will request a renewal again after 30 minutes. If the renewal fails, the client attempts again after half of the remaining time, for example, 15 minutes, then 7.5 minutes, and so on. If no renewal is given and the 60 minutes of the lease duration times out, the tunnel link terminates. To renew the connection the remote user must reconnect to the Security Gateway. Upon reconnection, an IKE renegotiation is initiated and a new tunnel created.

When the IP address is allocated from a predefined IP pool on the Security Gateway, the Security Gateway determines the IP lease duration period. The default is 15 minutes.

When using a DHCP server to assign IP addresses to users, the DHCP server’s configuration determines the IP lease duration. When a user disconnects and reconnects to the Security Gateway within a short period of time, it is likely that the user will get the same IP address as before.
No Office Mode - Secondary Tunnel Resilience

This release gives **No Office Mode** functionality for improved ATM connectivity.

**New features:**

- **No Office Mode** for Endpoint Security VPN for ATMs. Endpoint Security VPN does not require gateway Office Mode configuration and connects to the gateway without an Office Mode IP address.

  **Important** - If you change the client back to the regular mode after the **No Office Mode** client was installed, you must install the client again.

- Interoperability between **No Office Mode** and **Secondary Tunnel Resilience**. If Secondary Connect is enabled (two tunnels: primary active and secondary backup) and office mode is disabled, the secondary tunnel continues to work if the primary tunnel disconnects. The client automatically uses the updated topology the next time it connects to the gateway.

**Secondary Tunnel Resilience**

**Terminology:**

- **Primary Gateway**
  The gateway responsible for client configuration.

- **Secondary Gateway**
  The second gateway in a tunnel.

- **Default Gateway**: The gateway chosen as first to connect.

- **Roaming**
  A feature that detects tunnel disconnection status and tries to reconnect it.

**How Secondary Tunnel Resilience Works**

<table>
<thead>
<tr>
<th>Connection State</th>
<th>If Tunnel is Disconnected From:</th>
<th>Roaming Tries to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel to Primary Gateway (A) is connected</td>
<td>Primary Gateway (A)</td>
<td>Reconnect the tunnel.</td>
</tr>
<tr>
<td>Primary Gateway (A) and Secondary Gateway (B) are connected</td>
<td>Primary Gateway (A)</td>
<td>Reconnect the tunnel to the Primary Gateway (A). If roaming timeout is reached, the tunnel to the Primary Gateway (A) is disconnected. The Secondary Gateway (B) stays connected and is defined as the Primary Gateway. The tunnel to Gateway (A) is connected again with the encryption domain resource access, as Secondary Tunnel.</td>
</tr>
<tr>
<td>Primary Gateway and Secondary Gateway are connected</td>
<td>Secondary Gateway (B)</td>
<td>Reconnect the tunnel. Nothing changes in the client state.</td>
</tr>
</tbody>
</table>
Secure Configuration Verification (SCV)

In This Section:

- Check Point SCV Checks ............................................................................................................ 73
- Configuring the SCV Policy ........................................................................................................... 74
- Configuring SCV Enforcement ....................................................................................................... 74
- Configuring SCV Exceptions .......................................................................................................... 75
- Traditional Mode .......................................................................................................................... 75
- Installing and Running SCV Plugins on the Client ........................................................................ 75
- SCV Policy Syntax ......................................................................................................................... 76
- Deploying a Third Party SCV Check .............................................................................................. 97

Secure Configuration Verification (SCV) checks are DLLs (plug-ins) on the client that are invoked and enforced according to a policy. With SCV checks you have:

- Reports on the configuration of remote clients.
- Confirmation that the client complies with the organization’s security policy.
- Blocked connectivity from clients that do not comply.

**Note** - SCV is not supported in SecuRemote.

If you have SmartEndpoint-managed Endpoint Security VPN, you can use SCV checks or the Endpoint Security Compliance blade. If SCV is configured on the gateway then SCV is enforced. Clients report on their compliance status to the gateway.

Check Point SCV Checks

The default SCV checks (plug-ins) are part of the Endpoint Security VPN and Check Point Mobile for Windows installation.

- **OS Monitor** - Verifies Operating System version, Service Pack, and Screen Saver configuration (activation time, password protection, etc.).

- **HotFix Monitor** - Verifies that operating system security patches are installed, or not installed.

- **Group Monitor** - Verifies that the user logged into the operating system and is a member of specified Domain User Groups.

- **Process Monitor** - Verifies that a process is running, or not running, on the client machine (for example, that a file sharing application is not running, or that Anti-Virus is running).

- **Browser Monitor** - Verifies Internet Explorer version and configuration settings, such as Java and ActiveX options.

- **Registry Monitor** - Verifies System Registry keys, values, and their contents.

- **Anti-Virus Monitor** - Verifies that an Anti-Virus is running and checks its version. Supported: Norton, Trend Office Scan, and McAfee.

- **SCVMonitor** - Verifies the version of the SCV product, specifically the versions of the SCV DLLs installed on the client’s machine.
Secure Configuration Verification (SCV)

- **HWMonitor** - Verifies CPU type, family, and model.
- **ScriptRun** - Runs a specified executable on the client machine and checks the return code of the executable. For example, a script can check if a certain file is present on the client machine. It can perform additional configuration checks that you choose.
- **Windows Security Monitor** - Verifies that components monitored by Window Security Center are installed and enforced (for example, check if there is Anti-Virus installed and running). You can define which components you want to check.

**Configuring the SCV Policy**

An SCV Policy is a set of rules based on the checks that the SCV plug-ins provide. These rules decide whether a client is compliant. For example, to block a client that runs a file-sharing application, define a rule in the SCV Policy that verifies that this application is not running.

**Note** - The SCV check described in this example is among the pre-defined SCV checks included with the Security Management server. This check must be configured to check for the specific process.

- If the client passes all the SCV checks, the client is compliant.
- If the client fails one of the checks, it is not compliant.

Define the SCV policy through the `$FWDIR/conf/local.scv` file on the Security Management Server. The `local.scv` file is pushed to the Security Gateway when you do Install Desktop Policy.

**Important** - You must install the policy from the SmartDashboard or SmartConsole, as described here. If you use the command-line, the SCV checks are not included in the policy.

**Configuring SCV Enforcement**

The SCV Checks defined in the `local.scv` policy always run on the client. To let the gateway enforce access based on SCV results, configure the SCV settings on the gateway. For example, the gateway can immediately block non-compliant clients from connecting to the LAN.

To configure SCV Enforcement for the Gateways:

1. Open **Global Properties**:
   - **Pre-R80** - In SmartDashboard, open File > Policy > Global Properties.
   - **R80.x** - In SmartConsole, open Menu > Global Properties.
2. Open **Remote Access > Secure Configuration Verification (SCV)**.
3. Select **Apply Secure Configurations on Simplified Mode**.
   - This causes the gateway to verify client compliance.
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**
   - **Accept and log client’s connection**

If you block non-compliant clients, you can set up exceptions to allow the clients to download remediations.
5. Make sure that there is at least one rule in the firewall Rule Base that has the RemoteAccess VPN community object in the VPN column.
6. Click OK.
7. Install the policy.

Note - There are additional sections in the Secure Configuration Verification (SCV) page in Global Properties:
- Basic configuration verification on client’s machine
- Configuration Violation Notification on client’s machine
These settings are not supported for Remote Access Clients.

Configuring SCV Exceptions

Configure exceptions for hosts that can be accessed using selected services even if the client is not compliant.

You can allow a connection even if the client is non-compliant. For example, the client has to download the latest update or Anti-Virus version required by the SCV check.

To make exceptions for non-compliant remote clients:
1. Select the Apply Secure Configuration Verification on Simplified mode Firewall Policies option.
   The Exceptions button activates.
2. Click Exceptions.
   The Secure Configuration Verification Exceptions window opens.
3. Click Add.
4. Double-click None and select a host and service.
5. Click OK.

Traditional Mode

If you are using Traditional mode, configure SCV enforcement in the Rule Base.

To configure SCV enforcement in Traditional mode:
1. Open the Firewall Rule Base.
2. Add SCV Enforcement to the Client Encrypt rules.
3. Right-click Action and select Edit > Apply rule Only if Desktop Configuration is Verified.
4. Install the policy.

Installing and Running SCV Plugins on the Client

The SCV policy inspects elements of the client configuration, and returns the compliance status of the client. During installation, Remote Access Clients register their SCV DLLs as SCV plug-ins in the system registry.
When the Remote Access Clients connect to the gateway:

- Remote Access Clients download the SCV policy.
- The policy is enforced immediately and each time the client connects. The SCV checks run as defined in the SCV policy. The policy is also enforced if the client is disconnected.
- At regular intervals (by default, 20 seconds), the clients invoke the SCV DLLs defined in the SCV policy, and they report the client compliance status.
- If a client is non-compliant, a balloon notification appears. The behavior of the non-compliant client and access to the LAN is determined in the SCV enforcement settings on the gateway.

**SCV Policy Syntax**

The SCV Policy is configured on the Security Management Server in `$FWDIR/conf/local.scv`. The `local.scv` file is a policy file, containing sets, subsets and expressions.

In general, you can use the pre-defined checks (in the SCVNames section of the `local.scv` file) as templates and list the modified checks in the `SCVPolicy` section, without writing new SCV subsets.

**Sets and Sub-sets**

Each set has a purpose. For example, one set defines parameters, another defines actions for an event. Sets are differentiated by their names and hierarchy. Each set can have a sub-set, and each sub-set can have a sub-set of its own. Subsets can also contain logical expressions. Sets and sub-sets with more than one sub-set or condition are delimited by left and right parentheses `()`, and start with the set or sub-set name. Differentiate between sub-sets and expressions with a colon `:`.

**Sample Syntax:**

```plaintext
(SetName
   :SubSetName1 {
      :ExpressionName1_1 (5)
      :ExpressionName1_2 (false)
   }
   :SubSetName2 {
      :ExpressionName2_1 (true)
      :SubSetName2_1 {
         :ExpressionName2_1_1 (10)
      }
   }
)
```
Expressions

The expressions that you can use are set by the manufacturer. The names of the expressions are determined by the SCV check. The value of an expression is **true** or **false**, according to the result of an SCV check.

**Example:**

```plaintext
:browser_major_version (7)
```

This expression is a Check Point SCV check. It checks whether the version of the Internet Explorer browser installed on the client is 7.x. If the major version is 7, this expression is **true**.

**Grouping Expressions**

If several expressions appear one after the other, they are checked on AND logic. Only if all expressions are true, then the value of all of them together is true.

**Example:**

```plaintext
:browser_major_version (7)
:browser_minor_version (0)
```

If the version of Internet Explorer is 7 AND the minor version is 0 (version 7.0), the result is **true**. If the version is 6.0, the first expression is **false** and the second one is **true**: result is **false**.

**Influential Expressions**

Some expressions can influence the way in which others are evaluated.

**Example:**

```plaintext
:browser_major_version (7)
:browser_minor_version (0)
:browser_version_operand (">=")
```

The third expression influences the way that the first and second are evaluated. If the version of Internet Explorer is greater than or equal to (">=") 7.0, the result is **true**. If the version is 6.7, the result is **false**. If the version is 7.1, the result is **true**.

**Logical Sections**

Sometimes it is necessary to use a logical OR between expressions, instead of the default logical AND. Use labels to make this work. A label has a number, which differentiates between different OR sections.

```
begin_or (or#) - end (or#)
```

The **begin_or (or#)** label starts a section containing several expressions. The end of this section is marked by an **end (or#)** label. All expressions inside this section are evaluated on OR, resulting in one value for the section.
Example:

```plaintext
:begin_or(or1)
  :browser_major_version (9)
  :browser_major_version (10)
:end(or1)
```

This section checks if the version of Internet Explorer is 9 OR 10. If it is one or the other, the section is true.

**begin_and**

`begin_and (and#) - end (and#)`

The `begin_and (and#)` label starts a section to evaluate on AND. The end of this section is marked by an `end (and#)`. Use this label to nest AND sections inside OR sections.

Example:

If you consider 6.0 browsers to be insecure because of lack of components, and IE 8.x browser to be insecure because a security hole, you can define this section:

```plaintext
:begin_or (or1)
  :begin_and (and1)
    :browser_major_version (7)
    :browser_minor_version (0)
    :browser_version_operand (">=")
  :end (and1)
  :begin_and (and2)
    :browser_major_version (6)
    :browser_minor_version (0)
    :browser_version_operand ("<=")
  :end (and2)
:end (or1)
```

The first AND section checks if the version of IE >= 7.0. The second AND section checks whether the version of IE is <=6.0. The entire section is true if the version is greater than (or equal to) 7.0, OR lower than (or equal to) 6.0.
Expressions and Labels with Special Meanings

Some expressions and labels are reserved for specific purposes.

Example:

```plaintext
:browser_major_version (7)
:browser_minor_version (0)
:browser_version_operand ("=>")
:begin_admin (admin)
:send_log (alert)
:mismatchmessage ("The version of your Internet Explorer browser is old. For security reasons, users with old browsers are not allowed to access the network of the organization. Please upgrade your Internet Explorer to version 7.0 or higher.")
:end (admin)
```

**begin_admin**

`begin_admin (admin) - end (admin)`

This label is a section of actions for clients that were not checked by previous expressions in the subset (nothing relevant was installed on the client), or that returned `false` for all the expressions.

**mismatchmessage**

`mismatchmessage ("Message")`

This expression is used as part of the `begin_admin (admin) - end (admin)` section. It sets the message to show on the remote user’s desktop, to notify the user that the computer is not compliant. The message is shown only if the expression is `false`. We recommend that you use this text to tell the user what to do to resolve the issue.

**send_log**

`s`end_log (alert)`

This expression is for each SCV check. The value sets where the SCV check sends the logs.

- alert - A log with the non-compliant reason is sent to SmartView Tracker.
- log - The non-compliant reason is kept on the client.

The local.scv Sets

The `local.scv` policy file contains one set called `SCVObject`. This set must always be present and contain all the subsets for SCV checks and parameters. The required sub-sets are: `SCVNames`, `SCVEpsNames`, `SCVPolicy`, `SCVEpsPolicy`, and `SCVGlobalParams`.

**SCVNames**

The main SCV policy definition section. All the SCV checks and actions are defined. It does not set which SCV checks are active. In general, an SCV subset has a `type (plugin)` expression and a `parameters` subset.
Sample:

```plaintext
: (SCVCheckName1
   :type (plugin)
   :parameters {
     :Expression1 (value)
     :Expression2 (value)
     :begin_admin (admin)
     :send_log (alert)
     :mismatchmessage ("Failure Message")
     :end (admin)
   }
)
```

**SCVEpsNames**

Contains the SCV checks supported starting with R75 HFA1, for example, WindowsSecurityMonitor. Like the SCVNames section, it does not set which SCV checks are active. In general, an SCV subset has a **type (plugin)** expression and a **parameters** subset.

**SCVPolicy**

This section activates the SCV checks that are defined in **SCVNames**.

Sample:

```plaintext
:SCVPolicy {
   :(SCVCheckName1)
   :(SCVCheckName2)
}
```

Note - There is a space between the colon (:) and the opening parenthesis.

**SCVEpsPolicy**

This section activates the SCV checks that are defined in **SCVEpsNames**.

**SCVGlobalParams**

This section in **local.scv** defines global features for the SCV checks.
SCV Parameters

Typically, you will need to change only one or two parameters of a few default checks.

**Anti-Virus monitor**

This check is for the type and signature of Anti-Virus. It does not support `begin_or` or `begin_and`.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type (&quot;av_type&quot;)</td>
<td>Type of Anti-Virus. For example, ”Norton&quot;, &quot;VirusScan&quot;, “McAfee&quot;, &quot;OfficeScan&quot;, or “ZoneLabs&quot;.</td>
</tr>
<tr>
<td>Signature(x)</td>
<td>Required Virus definition file signature. The signature's format depends on the Anti-Virus type.</td>
</tr>
<tr>
<td></td>
<td>• Norton Antivirus example: ”&gt;=20031020” (format for Norton’s AV signature is ”yyyymmdd&quot;)</td>
</tr>
<tr>
<td></td>
<td>• TrendMicro OfficeScan example: ”&lt;650&quot;</td>
</tr>
<tr>
<td></td>
<td>• McAfee VirusScan example: (”&gt;404291&quot;) for a signature greater than 4.0.4291</td>
</tr>
<tr>
<td></td>
<td>• Zone Labs format: (”&gt;X.Y.Z”) where X = Major Version, Y = Minor Version, and Z = Build Number of the .dat signature file</td>
</tr>
</tbody>
</table>

**BrowserMonitor**

This check is only for Internet Explorer version, or only the browser settings for a certain zone. If none of these parameters appear, BrowserMonitor will not check the security settings of the restricted zones:

• restricted_download_signedactivex
• restricted_runactivex
• restricted_download_files
• restricted_java_permissions

If the parameter "browser_major_version" does not appear or is equal to zero, the IE version number is not checked.

BrowserMonitor does not support the `begin_or` or `begin_and`, and does not support the `admin` parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>browser_major_version(#)</td>
<td>Major version number of Internet Explorer. If this field does not exist in the local.scv file, or if this value is 0, the IE version will not be checked as part of the BrowserMonitor check.</td>
</tr>
<tr>
<td>browser_minor_version(#)</td>
<td>Internet Explorer minor version number.</td>
</tr>
<tr>
<td>browser_version_operand(&quot;=&quot;)</td>
<td>The operator used for checking the Internet Explorer’s version number.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>browser_version_mismatch_message</td>
<td>Message to be displayed for a non-verified configuration of Internet Explorer.</td>
</tr>
<tr>
<td>intranet_download_signedactivex (enable)</td>
<td>The maximum permission level that IE should have for downloading signed ActiveX controls from within the local Intranet.</td>
</tr>
<tr>
<td>intranet_runactivex (enable)</td>
<td>The maximum permission level that IE should have for running signed ActiveX controls from within the local Intranet.</td>
</tr>
<tr>
<td>intranet_download_files (enable)</td>
<td>The maximum permission level that IE should have for downloading files from within the local Intranet.</td>
</tr>
<tr>
<td>intranet_java_permissions (low)</td>
<td>The maximum security level that IE Explorer should have for running java applets from within the local Intranet.</td>
</tr>
<tr>
<td>trusted_download_signedactivex (enable)</td>
<td>The maximum permission level that IE should have for downloading signed ActiveX controls from trusted zones.</td>
</tr>
<tr>
<td>trusted_runactivex (enable)</td>
<td>The maximum permission level that IE should have for running signed ActiveX controls from trusted zones.</td>
</tr>
<tr>
<td>trusted_download_files (enable)</td>
<td>The maximum permission level that IE should have for downloading files from trusted zones.</td>
</tr>
<tr>
<td>trusted_java_permissions (medium)</td>
<td>The maximum security level that IE should have for running java applets from trusted zones.</td>
</tr>
<tr>
<td>internet_download_signedactivex (disable)</td>
<td>The maximum permission level that IE should have for downloading signed ActiveX controls from the Internet.</td>
</tr>
<tr>
<td>Internet_runactivex (disable)</td>
<td>The maximum permission level that IE should have for running signed ActiveX controls from the Internet.</td>
</tr>
<tr>
<td>internet_download_files (disable)</td>
<td>The maximum permission level that IE should have for downloading files from the Internet.</td>
</tr>
<tr>
<td>internet_java_permissions (disable)</td>
<td>The maximum security level that IE should have for running java applets from the Internet.</td>
</tr>
<tr>
<td>restricted_download_signedactivex (disable)</td>
<td>The maximum permission level that IE should have for downloading signed ActiveX controls from restricted zones.</td>
</tr>
<tr>
<td>restricted_runactivex (disable)</td>
<td>The maximum permission level that IE should have for running signed ActiveX controls from restricted zones.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>restricted_download_files</td>
<td>The maximum permission level that IE should have for downloading files from restricted zones.</td>
</tr>
<tr>
<td>restricted_java_permissions</td>
<td>The maximum security level that IE should have for running java applets from restricted zones.</td>
</tr>
<tr>
<td>send_log</td>
<td>Whether to send a log to Security Management server for specifying that the client is not verified: <strong>log</strong> or <strong>alert</strong>. Does not support <strong>begin_admin</strong>.</td>
</tr>
<tr>
<td>internet_options_mismatch_message</td>
<td>Mismatch message for the Internet Explorer settings.</td>
</tr>
</tbody>
</table>

### Groupmonitor

This checks that the logged on user belongs to the expected domain user groups.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;builtin\administrator&quot; (false)</td>
<td>A name of a user group. The user must belong to this group for the machine configuration to be verified.</td>
</tr>
</tbody>
</table>

### HotFixMonitor

This check is for Check Point Hotfixes. Some of these parameters may not appear at all, or may appear more than once in the **local.scv** file. These parameters can be in OR and AND sections.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HotFix_Number (true)</td>
<td>A number of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: &quot;823980(true)&quot; verifies that Microsoft’s RPC patch is installed on the operating system.</td>
</tr>
<tr>
<td>HotFix_Name (true)</td>
<td>The full name of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: &quot;KB823980(true)&quot; verifies that Microsoft’s RPC patch is installed on the operating system.</td>
</tr>
</tbody>
</table>

### HWMonitor

This check is for CPU details. It does not support the **begin_or** or **begin_and**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cputype (&quot;GenuineIntel&quot;)</td>
<td>The CPU type as described in the vendor ID string. The string has to be exactly 12 characters long. For example: &quot;GenuineIntel&quot;, or &quot;AuthenticAMD&quot;, or &quot;aaa bbb ccc &quot; where spaces count as a character.</td>
</tr>
<tr>
<td>cpufamily(6)</td>
<td>The CPU family.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

**OsMonitor**

This check is only for the operating system version and service pack, or only the screen saver configuration. If none of these parameters appear, **OsMonitor** will not check the system’s version and service pack on Windows XP platforms.

- major_os_version_number_xp
- minor_os_version_number_xp
- os_version_operand_xp
- service_pack_major_version_number_xp
- service_pack_minor_version_number_xp
- service_pack_version_operand_xp

If the parameter “enforce_screen_saver_minutes_to_activate” does not appear, the screen saver configuration is not checked.

**OsMonitor** does not support **begin_or** or **begin_and**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enforce_screen_saver_minutes_to_activate (3)</td>
<td>Time in minutes for the screen saver to activate. If the screen saver does not activate within this time period, then the client is not considered verified. In addition, the screen saver must be password protected.</td>
</tr>
<tr>
<td>screen_saver_mismatchmessage (“Your screen saver settings do not meet policy requirements”)</td>
<td>Mismatch message for the screen saver check. The screen saver will not be checked if the property “enforce_screen_saver_minutes_to_activate” does not appear, or if the time is set to zero.</td>
</tr>
<tr>
<td>major_os_version_number_xp (5)</td>
<td>Specifies the major version required for Windows XP operating systems to be verified.</td>
</tr>
<tr>
<td>minor_os_version_number_xp (1)</td>
<td>Specifies the minor version required for Windows XP operating systems to be verified.</td>
</tr>
<tr>
<td>os_version_operand_xp (“&gt;=”)</td>
<td>Operator for checking the operating system’s service pack on Windows XP</td>
</tr>
<tr>
<td>service_pack_major_version_number_xp (0)</td>
<td>Specifies the major service pack version required for Windows XP operating systems to be verified.</td>
</tr>
<tr>
<td>service_pack_minor_version_number_xp (0)</td>
<td>Specifies the minor service pack version required for Windows XP operating systems to be verified.</td>
</tr>
<tr>
<td>service_pack_version_operand_xp (“&gt;=”)</td>
<td>Operator for checking the operating system’s service pack on Windows XP.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>major_os_version_number_8 (6)</td>
<td>Specifies the major version required for Windows 8 operating systems to be verified.</td>
</tr>
<tr>
<td>minor_os_version_number_8 (2)</td>
<td>Specifies the minor version required for Windows 8 operating systems to be verified.</td>
</tr>
<tr>
<td>os_version_operand_8 (&quot;==&quot;)</td>
<td>Operator for checking the operating system’s service pack on Windows 8.</td>
</tr>
<tr>
<td>service_pack_major_version_number_8 (0)</td>
<td>Specifies the major service pack version required for Windows 8 operating systems to be verified.</td>
</tr>
<tr>
<td>service_pack_minor_version_number_8 (0)</td>
<td>Specifies the minor service pack version required for Windows 8 operating systems to be verified.</td>
</tr>
<tr>
<td>service_pack_version_operand_8 (&quot;&gt;=&quot;)</td>
<td>Operator for checking the operating system’s service pack on Windows 8.</td>
</tr>
<tr>
<td>major_os_version_number_7 (6)</td>
<td>Specifies the major version required for Windows 7 operating systems to be verified.</td>
</tr>
<tr>
<td>minor_os_version_number_7 (1)</td>
<td>Specifies the minor version required for Windows 7 operating systems to be verified.</td>
</tr>
<tr>
<td>os_version_operand_7 (&quot;==&quot;)</td>
<td>Operator for checking the operating system’s service pack on Windows 7.</td>
</tr>
<tr>
<td>service_pack_major_version_number_7 (0)</td>
<td>Specifies the major service pack version required for Windows 7 operating systems to be verified.</td>
</tr>
<tr>
<td>service_pack_minor_version_number_7 (0)</td>
<td>Specifies the minor service pack version required for Windows 7 operating systems to be verified.</td>
</tr>
<tr>
<td>service_pack_version_operand_7 (&quot;&gt;=&quot;)</td>
<td>Operator for checking the operating system’s service pack on Windows 7.</td>
</tr>
<tr>
<td>major_os_version_number_vista (6)</td>
<td>Specifies the major version required for Windows Vista operating systems to be verified.</td>
</tr>
<tr>
<td>minor_os_version_number_vista (0)</td>
<td>Specifies the minor version required for Windows Vista operating systems to be verified.</td>
</tr>
<tr>
<td>os_version_operand_vista (&quot;==&quot;)</td>
<td>Operator for checking the operating system’s service pack on Windows Vista.</td>
</tr>
<tr>
<td>service_pack_major_version_number_vista (1)</td>
<td>Specifies the major service pack version required for Windows Vista operating systems to be verified.</td>
</tr>
<tr>
<td>service_pack_minor_version_number_vista (0)</td>
<td>Specifies the minor service pack version required for Windows Vista operating systems to be verified.</td>
</tr>
</tbody>
</table>
### Parameter
**service_pack_version_operand_vista** (“>=”)
Operator for checking the operating system’s service pack on Windows Vista.

**os_version_mismatches** ("Please upgrade your operating system")
Message to be displayed in case of a non-verified configuration for the operating system’s version/service pack. The operating system’s version and service pack will not be checked if none of the parameters appear in the scv file.

---

### ProcessMonitor
This check is for process activity. It supports AND and OR sections.
It is based on the process name, with an additional hash check option for running processes.

\[
\text{ProcessName.exe}(\text{true} | \text{false})
\]

\[
\text{ProcessName.exe}(\text{true};<\text{SHA1 hash value}>)
\]
For example: calc.exe (true;9018A7D6CDBE859A430E8794E73381F77C840BE0)
If the value is true, the client is compliant if this process is running.
If the value is false, the client is compliant if the process is not running.

**Note** - Checking the SHA1 hash value can impact performance.

---

### RegMonitor
These checks are for the system registry. RegMonitor supports AND and OR sections.

**Note** - If the values of these parameters do not include the name of the registry hive, the HKEY_LOCAL_MACHINE hive is used by default. If you want to use another hive, you must explicitly use it in the value of the parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value (registry_value_path)</td>
<td>The path of a registry DWORD will be checked. The value should be an operator followed by a number, e.g. “Software\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\PatternVer&gt;=414”</td>
</tr>
<tr>
<td>string (registry_string_path)</td>
<td>The path of a registry string will be checked. The string’s value is compared to the given value, in the way that DWORDs are compared.</td>
</tr>
<tr>
<td>keynexist (registry_key_path)</td>
<td>The path of a registry key to be checked for exclusion. For the machine to be verified, the key should not exist.</td>
</tr>
<tr>
<td>keyexist (registry_key_path)</td>
<td>The path of a registry key to be checked for inclusion. For the machine to be verified, the key must exist.</td>
</tr>
</tbody>
</table>
Example: Script to check the version and service pack of Internet Explorer.

```plaintext
: (RegMonitor
  :type (plugin)
  :parameters {
    :begin_or (or1)
      :keynexist
        ("Software\Microsoft\Internet Explorer")
    :string
      ("Software\Microsoft\Internet Explorer\Version>=7")
    :begin_and (and1)
      :string
        ("Software\Microsoft\Windows\CurrentVersion\Internet Settings\MinorVersion=SP2")
    :string
      ("Software\Microsoft\Windows\CurrentVersion\Internet Settings\MinorVersion<=SP9")
    :end_and (and1)
    :begin_and (and2)
      :string
        ("Software\Microsoft\Internet Explorer\Version>=6.0")
    :string
      ("Software\Microsoft\Windows\CurrentVersion\Internet Settings\MinorVersion>=SP2")
    :string
      ("Software\Microsoft\Windows\CurrentVersion\Internet Settings\MinorVersion<=SP9")
    :end_and (and2)
    :end_or (or1)
    :begin_admin (admin)
      :send_log (alert)
      :mismatchmessage ("Your IE must be at least version 6.0 with SP2.")
    :end (admin)
  }
)
```

**SCVMonitor**

This check is for the version of SCV. It does not support `begin_and` or `begin_or`.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scv_version(&quot;&gt;=541000076&quot;)</td>
<td>SCV build-version of the SCV DLLs. This is not the same as the build number of Endpoint Security VPN. The string is an operator followed by the DLL’s version number in the format “vshhbbb”. For example, if you want the DLL version to be at least 54.1.0.220, the syntax should be: <code>scv_version (&quot;&gt;=541000220&quot;)</code></td>
</tr>
</tbody>
</table>
### ScriptRun

This check lets you run a specified executable on the client machine and checks the return code of the executable. For example, a script can check if a certain file is present on the client machine. It can perform additional configuration checks that you choose. If you do not enter a real script name, no script runs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>exe</code></td>
<td>The name and full path of the executable script on users’ machines. The extension can be any executable, for example, .pl, .bat.</td>
</tr>
<tr>
<td><code>script_run_cycle (#)</code></td>
<td>After how many cycles to run the script. A cycle is an interval defined in the global <code>scv_checks_interval</code>. It is 20 seconds by default and by default the script runs after every cycle (1).</td>
</tr>
<tr>
<td><code>run_as_admin [no]</code></td>
<td>Determines if the script runs with Administrator or User permissions. The default is “no”. If the value is “yes” the script runs with Administrator permissions.</td>
</tr>
<tr>
<td><code>run_timeout [#]</code></td>
<td>Time in seconds to wait for the executable to finish running. If it does not finish in the set time, the machine is considered not compliant. The default value is 0, no timeout.</td>
</tr>
</tbody>
</table>

If you enter invalid values for any of the attributes, for example letters instead of numbers, the computer that runs the script is considered not compliant.

### WindowsSecurityMonitor

This check uses Windows Security Center to monitor the status of computer security settings (for example, check if there is Anti-Virus installed and running). Configure it in the SCVEpsNames section and activate it in the SCVEpsPolicy section.

You can define which components you want to check and if you want to check for a specified product. It includes these checks:

- Network Firewall check
- Virus Protection check
- Spyware and Unwanted Software Protection check
- Windows Update check

For each component that you check, you can enter text for a mismatch message that users receive if they are non-compliant for that component.

You can configure a parameter to ignore failed results of the check if the Windows Security Center is not working.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>NetworkFirewallRequired</code></td>
<td>If it is set to true, a firewall is required. It queries the Windows Security Center to see if there is a Windows or third party firewall installed on the Endpoint machine.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NetworkFirewallInstalledPrograms</td>
<td>Possible values:</td>
</tr>
<tr>
<td></td>
<td>• any - Checks if there is any firewall installed on the endpoint machine (registered in the Windows Security Center).</td>
</tr>
<tr>
<td></td>
<td>• list of Firewalls separated by a &quot;;&quot; delimiter - Checks if one of the Firewalls on the list is installed on the endpoint machine.</td>
</tr>
<tr>
<td></td>
<td>• none - Disables the check.</td>
</tr>
<tr>
<td>VirusProtectionRequired</td>
<td>• If it is set to true, an Anti-Virus product is required. It queries the Windows Security Center to see if there is an Anti-Virus product installed and running on the Endpoint machine. It also checks that the Anti-Virus is up to date and that it has automatic scanning configured.</td>
</tr>
<tr>
<td>VirusProtectionInstalledPrograms</td>
<td>Checks which Anti-Virus program is installed. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• any - Checks if there is any Anti-Virus installed on the endpoint machine (registered in the Windows Security Center).</td>
</tr>
<tr>
<td></td>
<td>• list of Anti-Virus products separated by a &quot;;&quot; delimiter - Checks if one of the Anti-Virus products on the list is installed, on the endpoint machine.</td>
</tr>
<tr>
<td></td>
<td>• none - Disables the check</td>
</tr>
<tr>
<td>SpywareProtectionRequired</td>
<td>If it is set to true, an Anti-Spyware protection and Unwanted Software product is required. It queries the Windows Security Center to see if there is an Anti-Spyware product installed on the Endpoint machine. It also checks that the Anti-Spyware is up to date and that it has automatic scanning configured.</td>
</tr>
<tr>
<td>SpywareProtectionInstalledPrograms</td>
<td>Checks if there is an Anti-Spyware product installed on the Endpoint machine. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• any - Checks if there is any Anti-Spyware installed on the endpoint machine (registered in the Windows Security Center).</td>
</tr>
<tr>
<td></td>
<td>• list of Anti-Spyware products separated by a &quot;;&quot; delimiter - Checks if one of the Anti-Spyware products on the list is installed on the endpoint machine.</td>
</tr>
<tr>
<td></td>
<td>• none - Disables the check</td>
</tr>
<tr>
<td>WindowsUpdateRequired</td>
<td>Queries the Windows Security Center to see if the Endpoint machine has Windows Automatic Updates configured. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• true - Enables the check.</td>
</tr>
<tr>
<td></td>
<td>• false - Disables the check.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>&lt;CheckName&gt;</code>MismatchMessage</td>
<td>For each check, enter the message that users get if they are not compliant. For example, &quot;You do not have a Firewall enabled. Enable a firewall or contact your administrator for help.&quot;</td>
</tr>
</tbody>
</table>
| PassCheckWhenSecurityCenterIsUnavaiable | Can override the WindowsSecurityMonitor checks if the Windows Security Center is not working. Possible values:  
  - `true` - If a client fails the WindowsSecurityMonitor checks because of an internal error of the Microsoft WMI service (which reports from Windows Security Center), the fail is ignored. The client is considered compliant and can access the gateway.  
  - `false` - [default] If there is an internal error of the Microsoft WMI service and a client fails the WindowsSecurityMonitor checks, it is considered non-compliant and cannot access the gateway. For security reasons, this is the default. |
| MinutesForWscsvToStart(x) | If a client is not compliant because the wscsvc service did not start, it will be considered compliant for x minutes. If the wscsvc service does not start after x minutes, the client will be non compliant. Minutes are counted from when the computer boots. Enter a value (in minutes) for x. |

**Finding Exact Product Names**

You can include lists of products in the WindowsSecurityMonitor check for these parameters:  
- NetworkFirewallInstalledPrograms  
- VirusProtectionInstalledPrograms  
- SpywareProtectionInstalledPrograms  

You must write the names of the products the same as they are shown in the Windows Management Instrumentation Tester tool. The product only shows if it is installed on that computer.

**To find names in the Windows Management Instrumentation Tester tool:**

1. Open the command prompt as an administrator and enter `wbemtest`. The Windows Management Instrumentation Tester opens.  
2. Click Connect.  
3. In the **Namespace** field enter `root\SecurityCenter` and click Connect. In Windows 7 some of the products are registered in `root\SecurityCenter2`.  
4. Click **Enum Instances**.  
5. In the **Class Info** Window, enter the class of product without spaces:  
   - AntiVirusProduct  
   - FirewallProduct  
   - AntySpywareProduct (only on Windows 7 or Vista)  
6. Double click an instance that shows in the **Query Results**.
7. In the **Object editor** window, scroll down to the **displayName** property. Copy the name listed and use that in the parameters of the check.

**Example of a WindowsSecurityMonitor configuration**

```plaintext
SCVEpsNames {
    : (WindowsSecurityMonitor
        :type (plugin)
        :parameters (
            :VirusProtectionRequired (true)
            :VirusProtectionRequiredMismatchMessage
            :VirusProtectionInstalledPrograms ("Trend Micro OfficeScan Antivirus;Kaspersky Anti-Virus")
            :VirusProtectionInstalledProgramsMismatchMessage
            :VirusProtectionInstalledProgramsMismatchMessage
            :WindowsUpdateRequired (true)
            :WindowsUpdateRequiredMismatchMessage
            :SpywareProtectionRequired (true)
            :SpywareProtectionRequiredMismatchMessage
            :SpywareProtectionInstalledPrograms ("none")
            :SpywareProtectionInstalledProgramsMismatchMessage
            :SpywareProtectionInstalledProgramsMismatchMessage
            :NetworkFirewallRequired (true)
            :NetworkFirewallRequiredMismatchMessage
            :NetworkFirewallInstalledPrograms ("Kaspersky Anti-Virus")
            :NetworkFirewallInstalledProgramsMismatchMessage
            :NetworkFirewallInstalledProgramsMismatchMessage
        )
    )
}
```

**SCV Global Parameters**

There are global features for the SCV checks.

**Disconnect When Not Verified**

This feature lets you disconnect the client if it becomes non-compliant while connected to the VPN.

2. In the **SCVGlobalParams** section, set the value of the **disconnect_when_not_verified** parameter:
   - **true** - A connected, non-compliant client is automatically disconnected from the VPN. A notification is shown to the user.
   - **false** - A connected, non-compliant client stays connected to the VPN. This is default.

**Not Verified Script**

This feature lets you configure script-running if a client becomes non-compliant. If you can run scripts on non-compliant clients, you can use them to send remediations. For example, you can run a script that install an Anti-Virus, or a script that opens an HTML page with a link to the remediation.

2. In the **SCVGlobalParams** section, find the **not_verified_script**.

3. In the value, put the name of the script.
   - You must supply the script to the client computers.
   - If necessary, you must make sure it is in the search path.

4. Set the value of the **not_verified_script_run_show** parameter:
   - **true** - The user will see the script running.
   - **false** - The script run will be hidden (default).

5. Set the value of the **not_verified_script_run_admin** parameter:
   - **true** - The script will run under the Remote Access Clients Service account with administrator permissions, even if the user does not have these permissions.
   - **false** - The script will run under the local user account permissions (default). If administrator permissions are necessary, the script will fail.

6. Set the value of the **not_verified_script_run_always** parameter:
   - **true** - The script runs every time the client becomes non-compliant.
   - **false** - The script runs the first time that the client becomes non-compliant. (default)

**SCV Intervals**

This feature lets you change the default interval after which the SCV checks run. By default, the interval is 20 seconds, so checks run at 20 second intervals.

To change the interval in the global parameters:


2. In the **SCVGlobalParams** section, set the value of the **scv_checks_interval** parameter to a desired number of seconds.
   - If you set the value to 0 or enter an invalid value, such as a letter, the interval will be the default 20 seconds.

3. Install the Desktop Policy in SmartDashboard or R80.x SmartConsole.
   - The change takes effect when a client connects.

**Allow Clients without Firewall**

The Skip firewall enforcement option lets you allow gateway connections from clients that do not have a firewall enforced, such as Check Point Mobile for Windows. By default, this option is disabled so that firewall enforcement is required as part of the SCV check.

*Notes*

- This parameter is not related to the `NetworkFirewallRequired` parameter in the Window Security Monitor check.

- Endpoint Security VPN ignores the parameter `skip_firewall_enforcement_check`. It always checks for firewall enforcement.

To enable Skip firewall enforcement in the global parameters:


2. In the **SCVGlobalParams** section, set the value of the **skip_firewall_enforcement_check** parameter to **true**.
3. Install the Desktop Policy in SmartDashboard or R80.x SmartConsole. The change takes effect when a client connects.

**Allow Clients without SCV**

The *Allow non SCV clients* option lets you allow gateway connections from clients that do not have SCV, such as SecuRemote. The setting does not take effect if the endpoint client does have SCV. Therefore, if this option is configured, the gateway still requires SCV compliance from Check Point Mobile for Windows or Endpoint Security VPN before they can access resources behind the gateway. By default, this option is disabled.

To enable Allow non SCV Clients in the global parameters:

2. In the `SCVGlobalParams` section, set the value of the `allow_non_scv_clients` parameter to `true`.
3. Install the Desktop Policy in SmartDashboard or R80.x SmartConsole. The change occurs when a client connects.

**Enforcing the SCV Checks**

To enforce a specified SCV check from versions before E75.10:
- Set the SCV parameters in `SCVNames`.
- Include the name of the check in `SCVPolicy`.

To enforce SCV checks from version E75.10 or later, such as `WindowsSecurityMonitor`:
- Set the SCV parameters in `SCVEpsNames`.
- Include the name of the check in `SCVEpsPolicy`.

**Sample local.scv Configuration File**

You must maintain the same indentation format.

```plaintext
(SCVObject
 :SCVNames (  
 : (user_policy_scv  
 :type (plugin)
 :parameters (  
 )  
)
 : (BrowserMonitor  
 :type (plugin)
 :parameters (  
 :browser_major_version (5)
 :browser_minor_version (0)
 :browser_version_operand (">=")
 :browser_version_mismatchmassage ("Please upgrade your Internet browser.")
 :intranet_download_signedactivex (disable)
 :intranet_runactivex (disable)
 :intranet_downloadfiles (disable)
 :intranet_java_permissions (disable)
 :trusted_download_signedactivex (disable)
 ))
```
settings do not meet policy requirements. Please check the following settings:

1. In your browser, go to Tools -> Internet Options -> Security. For each Web content zone, select custom level and disable the following items: Download signed ActiveX, Run ActiveX Controls, Download Files and Java Permissions.

2. Right click on your desktop and select properties.
3. Under Wait choose 3 minutes and check the Password Protection box.

Major OS Version Number_9x: 4
Minor OS Version Number_9x: 10
OS Version Operand_9x: ">="
Service Pack Major Version Number_9x: 0
Service Pack Minor Version Number_9x: 0
Service Pack Version Operand_9x: ">="

Major OS Version Number_NT: 4
Minor OS Version Number_NT: 0
OS Version Operand_NT: "=="
Service Pack Major Version Number_NT: 5
Service Pack Minor Version Number_NT: 0
Service Pack Version Operand_NT: ">="

Major OS Version Number_2K: 5
Minor OS Version Number_2K: 0
OS Version Operand_2K: "=="
Service Pack Major Version Number_2K: 0
Service Pack Minor Version Number_2K: 0
Service Pack Version Operand_2K: ">="

Major OS Version Number_XP: 5
Minor OS Version Number_XP: 1
OS Version Operand_XP: "=="
Service Pack Major Version Number_XP: 0
Service Pack Minor Version Number_XP: 0
Service Pack Version Operand_XP: ">="

Major OS Version Number_2003: 5
Minor OS Version Number_2003: 2
OS Version Operand_2003: "=="
Service Pack Major Version Number_2003: 0
Service Pack Minor Version Number_2003: 0
Service Pack Version Operand_2003: ">="

OsMonitor

type (plugin)
:parameters (os_version_mismatchmessage ("Please upgrade your operating system."))
enforce_screen_saver_minutes_to_activate (3)
screen_saver_mismatchmessage ("Your screen saver settings do not meet policy requirements. Please check the following settings:

1. Right click on your desktop and select properties.
2. Select the Screen Saver tab. Under Wait choose 3 minutes and check the Password Protection box.

Send Log (alert)
major_os_version_number_9x (4)
minor_os_version_number_9x (10)
os_version_operand_9x (">=")
service_pack_major_version_number_9x (0)
service_pack_minor_version_number_9x (0)
service_pack_version_operand_9x (">=")
major_os_version_number_nt (4)
minor_os_version_number_nt (0)
os_version_operand_nt ("==")
service_pack_major_version_number_nt (5)
service_pack_minor_version_number_nt (0)
service_pack_version_operand_nt (">=")
major_os_version_number_2k (5)
minor_os_version_number_2k (0)
os_version_operand_2k ("==")
service_pack_major_version_number_2k (0)
service_pack_minor_version_number_2k (0)
service_pack_version_operand_2k (">=")
major_os_version_number_xp (5)
minor_os_version_number_xp (1)
os_version_operand_xp ("==")
service_pack_major_version_number_xp (0)
service_pack_minor_version_number_xp (0)
service_pack_version_operand_xp (">=")
major_os_version_number_2003 (5)
minor_os_version_number_2003 (2)
os_version_operand_2003 ("==")
service_pack_major_version_number_2003 (0)
service_pack_minor_version_number_2003 (0)
service_pack_version_operand_2003 (">=")
)
))
(ProcessMonitor

type (plugin)
:parameters {
  :calc.exe (false)
  :begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("Please make sure calc.exe is not running!")
  :end (admin)
}

:groupmonitor
:type (plugin)
:parameters {
  :begin_or (or1)
  :begin_and (1)
  :"builtin\administrator" (false)
  :"BUILTIN\Users" (true)
  :end (1)
  :begin_and (2)
  :"builtin\administrator" (true)
  :"BUILTIN\Users" (false)
  :end (and2)
  :end (or1)
  :begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("You are using SecureClient with a non-authorized user.\nMake sure you are logged on as an authorized user.")
  :securely_configured_no_active_user (false)
  :end (admin)
}

:HotFixMonitor
:type (plugin)
:parameters {
  :147222 (true)
  :begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("Please install security patch Q147222.")
  :end (admin)
}

:AntiVirusMonitor
:type (plugin)
:parameters {
  :type ("Norton")
  :Signature (">=20020819")
  :begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("Please update your AntiVirus (use the LiveUpdate option).")
  :end (admin)
}

:HWMonitor
:type (plugin)
:parameters {
  :cputype ("GenuineIntel")
  :cpumodel ("9")
  :cpufamily ("6")
  :begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("Your machine must have an\nIntel(R) Centrino(TM) processor installed.")
  :end (admin)
Secure Configuration Verification (SCV)

: (ScriptRun
   :type (plugin)
   :parameters (
      :exe ("VerifyScript.bat")
      :begin_admin (admin)
      :send_log (alert)
      :mismatchmessage ("Verification script has determined that your configuration does not meet policy requirements.")
   )
)

: (RegMonitor
   :type (plugin)
   :parameters (
      :value ("Software\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc\PatternVer>=414")
      :begin_admin (admin)
      :send_log (alert)
      :mismatchmessage ("Please update your AntiVirus (use the LiveUpdate option).")
   )
)

: (SCVMonitor
   :type (plugin)
   :parameters ( 
      :scv_version ("54014")
      :begin_admin (admin)
      :send_log (alert)
      :mismatchmessage ("Please upgrade your Secure Configuration Verification products package.")
   )
)

: (sc_ver_scv
   :type (plugin)
   :parameters ( 
      :Default_SecureClientBuildNumber (52032)
      :Default_EnforceBuildOperand ("==")
      :MismatchMessage ("Please upgrade your SecureClient.")
      :EnforceBuild_9X_Operand (">=")
      :SecureClient_9X_BuildNumber (52030)
      :EnforceBuild_NT_Operand ("==")
      :SecureClient_NT_BuildNumber (52032)
      :EnforceBuild_2K_Operand (">=")
      :SecureClient_2K_BuildNumber (52032)
      :EnforceBuild_XP_Operand (">=")
      :SecureClient_XP_BuildNumber (52032)
   )
)

:SCVEpsNames ( 
   : (WindowsSecurityMonitor
      :type (plugin)
      :parameters ( 
         :VirusProtectionRequired (true)
         :VirusProtectionRequiredMismatchMessage ("Please verify that your virus protection is up to date and virus scanning is on.")
         :VirusProtectionInstalledPrograms ("Kaspersky Anti-Virus")
         :VirusProtectionInstalledProgramsMismatchMessage ("Please verify that the anti-virus of Kaspersky Anti-Virus is installed.")
         :WindowsUpdateRequired (false)
Deploying a Third Party SCV Check

You can integrate a third party SCV check into the Remote Access Clients SCV policy. To use a third party SCV check, create a DLL according to the OPSEC SCV Specifications.

We recommended that you add the DLL to an MSI package with the Check Point MSI Packaging tool utility (“Editing an MSI Package with CLI” on page 24). When clients install the MSI they automatically get the DLL.

You can also add the check to existing client installations manually.


To activate a third party SCV check:

1. Create a DLL file according to the OPSEC SCV Specifications.
2. Edit the `$FWDIR/conf/local.scv` file on the Security Management Server to include the third party check.
3. Install the Desktop Policy in SmartDashboard or R80.x SmartConsole.
4. Add a third party SCV DLL file to an MSI package. Use the Check Point MSI Packaging tool commands to edit the MSI package and add, remove, and overwrite a third party plug-in file.
The Configuration File

In This Section:

- Editing the TTM File ...................................................................................................... 98
- Centrally Managing the Configuration File ................................................................. 98
- Understanding the Configuration File ......................................................................... 99

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 Remote Access Clients. 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:
   
   NAME = conf/trac_client_1.ttm; DST = conf/trac_client_1.ttm;
   
   This copies the file to the Remote Access Clients 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**

Monitoring and Troubleshooting

In This Section:

SmartView Tracker and Remote Access Clients ...................................................... 101
Collecting Logs ........................................................................................................... 102
Remote Access Clients Files ...................................................................................... 103
Error Messages .......................................................................................................... 105
Configuring No-Router Environments ..................................................................... 105
Connection Terminates ............................................................................................. 105
Troubleshooting the Firewall .................................................................................... 106
Troubleshooting SCV .................................................................................................. 114
Traffic Dropped for Anti-spoofing .............................................................................. 115
MEP ............................................................................................................................. 115

SmartView Tracker and Remote Access Clients

To see alerts from Remote Access Clients:

1. Open SmartView Tracker.


<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Time</th>
<th>Interface</th>
<th>Origin</th>
<th>Type</th>
<th>Action</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11Nov2008</td>
<td>11:00:28</td>
<td>Desktop</td>
<td>Alaska_cluster</td>
<td>Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>11Nov2008</td>
<td>22:10:46</td>
<td>Desktop</td>
<td>Alaska_cluster</td>
<td>Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>12Nov2008</td>
<td>4:04:16</td>
<td>Desktop</td>
<td>California_GW</td>
<td>Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>14Nov2008</td>
<td>3:42:05</td>
<td>Desktop</td>
<td>California_GW</td>
<td>Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>14Nov2008</td>
<td>4:12:00</td>
<td>Desktop</td>
<td>Delaware_cluster</td>
<td>Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>15Nov2008</td>
<td>10:03:59</td>
<td>Desktop</td>
<td>Georgia_GW</td>
<td>Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>19Nov2008</td>
<td>13:07:47</td>
<td>Desktop</td>
<td>Georgia_GW</td>
<td>Alert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>22Nov2008</td>
<td>19:46:09</td>
<td>Desktop</td>
<td>California_GW</td>
<td>Alert</td>
<td>Drop</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>22Nov2008</td>
<td>19:46:09</td>
<td>Desktop</td>
<td>California_GW</td>
<td>Alert</td>
<td>Drop</td>
<td></td>
</tr>
</tbody>
</table>
3. Double-click an item to open the **Record Details** window and see more data.

<table>
<thead>
<tr>
<th>Log info</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Action</td>
</tr>
<tr>
<td>Time</td>
<td>Rule</td>
</tr>
<tr>
<td>Number</td>
<td>Current Rule Number</td>
</tr>
<tr>
<td>Type</td>
<td>Rule Name</td>
</tr>
<tr>
<td>Origin</td>
<td>User</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic</th>
<th>More</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Information</td>
</tr>
<tr>
<td>Service</td>
<td>message: Failed to load Desktop Security Policy Standard site_name: Alaska</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>Source Port</td>
<td></td>
</tr>
</tbody>
</table>

Collecting Logs

Each client can collect its logs into a cab file. You can configure clients to send logs to you. When a user does the Collect Logs action, the cab file is sent to your email address.

For SmartDashboard-managed clients, 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.

```ruby
: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.

You will get the email after the user does Collect Logs.

**To collect logs on a client:**
1. Right-click the client icon 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.

**Troubleshooting Log Collection**

- If a client is not configured to send the logs to an email address, you can find the cab file at: `\%temp%\trac\trlogs_timestamp.cab`

**Remote Access Clients Files**

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

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminMode.bat</td>
<td>Opens the client with the Administrator tab, to generate a new MSI package.</td>
<td></td>
</tr>
<tr>
<td>DLLs</td>
<td></td>
<td>Some DLLs install SCV checks on client computers.</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>cpmsi_tool.exe</td>
<td>CLI for updating an MSI.</td>
<td>This is the same tool that is launched from the Administrator tab, when the client is in AdminMode.</td>
</tr>
<tr>
<td>trac.exe</td>
<td>The Remote Access Clients CLI ([&quot;Remote Access Clients Command Line&quot; on page 122].</td>
<td></td>
</tr>
<tr>
<td>TracSrvWrapper.exe</td>
<td>The Remote Access Clients service.</td>
<td></td>
</tr>
<tr>
<td>update_config_tool.exe</td>
<td>CLI of the update tool.</td>
<td>If you want to change an MSI package after you generated it, you must use the CLI. It has options that are not in the GUI to add and remove files from the MSI.</td>
</tr>
<tr>
<td>TRAC.cab</td>
<td>The client MSI and other installation files on the gateway.</td>
<td>In most cases, this file is not on client computers.</td>
</tr>
<tr>
<td>desktop_policy.ini</td>
<td>The desktop policy.</td>
<td></td>
</tr>
<tr>
<td>Filename</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</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.</td>
</tr>
<tr>
<td>vna.sys</td>
<td>driver</td>
<td></td>
</tr>
<tr>
<td>cpgina.log, cpplap.log</td>
<td>Logs for Remote Access Clients support for Windows SDL by GINA and PLAP.</td>
<td></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.</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.bat</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 batch file on a client to run the collection and see the verbose output of the log collections.</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.</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 Remote Access Clients client (for example, in a lab environment).

To configure Remote Access Clients to operate without a router:

1. In SmartDashboard, open the properties of the Remote Access Clients gateway.
2. Open IPSEC VPN >Office Mode:
3. Select the Multiple Interfaces option: Support connectivity enhancement for gateways with multiple external interfaces.

Connection Terminates

If all client connections stop at a given interval (default is 15 minutes), the DHCP server might be configured to use the lowest IP lease timeout.
To repair this issue:
1. In SmartDashboard or R80.x SmartConsole, open the Gateway Properties window of the Remote Access Clients gateway.
2. Open IPSec VPN > Office Mode.
3. Click Offer Office Mode to group or Allow Office Mode to all users.
4. Click Optional Parameters.
5. Increase the value of IP lease duration.
6. Click OK.
7. Install Policy.

Troubleshooting the Firewall

To troubleshoot the firewall, you can use these tools:

- Windows service query (sc query)
- The command line packet monitoring utility (PacketMon.exe)

Using the Windows Service Query

You can use the Windows service query (sc query) to see the status of the firewall in the desktop policy.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>vsdatant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Check Point service for the desktop policy firewall.</td>
</tr>
<tr>
<td>Syntax</td>
<td><code>sc query vsdatant</code></td>
</tr>
</tbody>
</table>
| Example Output | STATE : 4 Running  
<STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN> |

Desktop Firewall Monitoring

Packet monitoring has two components, a user-mode utility (PacketMon.exe) and a Kernel component (implemented in VSDATANT.SYS). PacketMon must only be used for debugging purposes. Running PacketMon strongly impacts the performance of VSDATANT.

PacketMon:

- Analyzes command-line input parameters.
- Compiles an INSPECT assembly code.
- Uploads the INSPECT assembly code to VSDATANT.SYS
- Samples VSDATANT.SYS for new packet inspection data.
- Shows packet data on the screen or redirects to a file (in SNOOP format).
- Stops packet inspection when terminated by user.
**VSDATANT:**

- Initializes input and output buffers.
- Runs each incoming and outgoing packet through the INSPECT virtual machine.
- Runs each accepted packet (if –d option was not specified) or each dropped packet (if –d option was specified) through the INSPECT virtual machine.
- Copies packet data into user-mode buffers when instructed to by PacketMon.
- De-initializes the input and output buffers and stops packet inspection when instructed to by PacketMon.

Use **PacketMon.exe**, to inspect traffic handled by the Desktop Firewall blade. When run without parameters, the utility captures all inbound and outbound packets. The application first analyzes and validates the input parameters.

If an error occurs, this usage message shows:

```

-e expr: filters packets according to the given expr regular expression
-l len: limits packet capture length to the given len bytes
-m mask: captures packets according to the given mask
mask can be combination of:
  i - incoming packets (while entering the firewall)
  I - incoming packets (while leaving the firewall)
  o - outgoing packets (while entering the firewall)
  O - outgoing packets (while leaving the firewall)
-x offset[,len]: prints packet data starting from the given offset and
for an optional number of bytes (len). offset is the offset from the
beginning of the IP header

len can be used to limit the amount of bytes printed. If omitted will
print the whole packet from the given offset to its end
-o file: write output to the given file (in snoop file format)
-ci count: captures count number of incoming packets and exits
-co count: captures count number of outgoing packets and exits
-I: shows interface numbers instead of names
-f filter_file: filters packets according to the regular expression given
in the filter_file file
-f -: filters packets according to the regular expression given in the
standard input
  Ctrl-Z+<Enter> at a new line to stop stdin input
-d: shows only dropped packets
-r: prints relevant rule (if found)
-T: prints time stamp
-h: shows this help message
-i: flushes standard output
-t: do not include fwmonitor.def file automatically
```

**Running PacketMon**

1. Open a command prompt
2. Change directory to the E80.71 installation folder.
3. Run: `packetmon`.

**Note** -

- You can only run one instance of `PacketMon.exe` at a time.
- To stop packet monitoring, press Ctrl-c.
### Command Syntax in Detail

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-h</code></td>
<td>Shows command usage&lt;br&gt;Purpose: <code>packetmon -h</code>&lt;br&gt;Example: <code>packetmon -h</code></td>
</tr>
<tr>
<td><code>-e expr</code></td>
<td>Filters packets according to the given INSPECT expression <code>{expr}</code>&lt;br&gt;Purpose: <code>packetmon -e &quot;tcpport(23), accept;&quot;</code>&lt;br&gt;Example: <code>packetmon -e &quot;tcpport(23), accept;&quot;</code>&lt;br&gt;Default: If the <code>-e</code> option is not given, all packets are captured. This option is the same as running: <code>packetmon -e &quot;accept;&quot;</code>&lt;br&gt;Note: The <code>-e</code> option cannot be used with the <code>-f</code> option.&lt;br&gt;See also the <code>-t</code> option.</td>
</tr>
</tbody>
</table>
| `-f file` | Filters packets according to INSPECT expressions in a given file. To use pre-defined INSPECT macros, the given file must include the `'#include "fwmonitor.def"'` directive.<br>Purpose: To use pre-defined INSPECT macros, the given file must include the `'#include "fwmonitor.def"'` directive.<br>Note: The `-f` option cannot be used with the `-e` option.<br>Example: `packetmon -f inspect.dat`<br>**Inspect.dat contents:**<br>`#include "fwmonitor.def"
tcpport(23), accept;` |
| `-f -` | Filters packets according to INSPECT expressions given in the standard input. To use pre-defined INSPECT macros, the input must include the directive: `'#include "fwmonitor.def"'`<br>Purpose: To use pre-defined INSPECT macros, the input must include the directive: `'#include "fwmonitor.def"'`<br>Note: The `-f -` option can not be used with the `-e` option.<br>Example: `packetmon -f -`<br>To stop command input and start packet inspection based on the given input, enter `Ctrl-Z+<Enter>` at a new line. |
### Standard input contents:
```
#include "fwmonitor.def"
tcpport(23), accept;
Ctrl-Z+<Enter>
```

### -t
**Purpose**
The `fwmonitor.def` file includes all the INSPECT predefined macros you can use with the `-e` option. `Fwmonitor.def` is included automatically when you use the `-e` option.

If you want to define new macros with the same name as those defined in `fwmonitor.def`, use the `-t` option to exclude `fwmonitor.def`, and include your own definition file.

### -l len
**Purpose**
Limits packet capture length to the given `len` bytes. Note: `len` indicates number of bytes to capture starting at the IP header. Regardless of the `len` value, the MAC header is always captured.

**Example**
```
packetmon -l 20
```

**Default**
If the `-l` option is not given, all packet data is captured

**Comment**
- This option is useful if you have to debug highly sensitive communication data. The options lets you capture only the headers of a packet (e.g. IP and TCP header) while omitting the actual sensitive payload. You can debug the communication without seeing the actual data transmitted.
- On computers experiencing a heavy load, you can use this option to reduce the file size by omitting the payload. The packetmon utility uses a buffer to transfer the packets from Kernel to user space. Reducing the packet length slows the rate at which the buffer fills.
| **-m mask** |  |
| Purpose | By default packetmon captures packets before and after firewall inspection. The `-m` option lets you to specify capture on:  
- `i`  
  Inbound packets before firewall inspection.  
- `I`  
  Inbound packets after firewall inspection.  
- `o`  
  Outbound packets before firewall inspection  
- `O`  
  Outbound packets after firewall inspection  
The mask can be a combination of the above. |
| Example | `packetmon -m IO` |
| Default | Not specifying the `-m` option is the same as running `packetmon -m iIoO` |

| **-x offset [, len]** |  |
| Purpose | The `-x` option lets you print a packet’s raw data. The value is an offset from the beginning of the IP header. You can also use the `len` option to limit the data printed to the standard output (screen or file). If `len` is specified, data is printed from the offset for `len` number of bytes. If `len` is not specified, data is printed from the given offset until the end of the packet.  
Note: Using the `-l` option can change the behavior of the `-x offset` option. Less data is printed to screen. |
| Examples | `packetmon -x 20`  
`packetmon -x 0,28` |
| Default | Not specifying the `-x` options prevents a packet’s raw from being printed to screen. |

| **-o file** |  |
| Purpose | The `-o` option saves raw packet data to a file. The file format used is the same format used by tools like snoop (RFC 1761). This file format can be examined using Wireshark, Snoop, tcpdump, or tools similar to these. |
| Example | `packetmon -o capture.cap` |
### -ci count / -co count

**Purpose**
This option limit the number of packets being captured. This is useful when you need to troubleshoot a firewall handling large amounts of traffic.

- **-ci**
  Defines how many inbound packets to capture
- **-co**
  Defines how many outbound packets to capture

**Examples**
- `packetmon -ci 5`
- `packetmon -ci 3 -co 10`

### -I

**Purpose**
To avoid long interface names, this option prints the index of the interface on which the packet was received or sent. After the packet capture is stopped, a list of all interfaces (index and names) is printed.

**Example**
- `packetmon -I`

**Default**
If the option is not specified, the interface name is printed.

### -d

**Purpose**
This option shows packets dropped by the firewall. Use this option when you need to locate a packet missing from the output.

**Example**
- `packetmon -d`

**Default**
Without this option, packetmon shows packets before they pass through the FW engine (i/o) and packets accepted by the FW engine (I/O). Packet that are dropped are not shown.

### -r

**Purpose**
If a packet is dropped or accepted because of a rule, this option prints the name and the ID of the rule.

**Example**
- `packetmon -r`

### -T

**Purpose**
This option prints the time stamp for each packet.

**Example**
- `packetmon -T`
### Monitoring and Troubleshooting

**-i**

**Purpose**
Use this option to make sure that captured data for each packet is written immediately to the standard output (screen or file). This is useful if you want to kill a running `packetmon` capture process or be sure that all data is written to a file.

**Example**
`packetmon -i > output.log`

---

**Major INSPECT macros supported by PacketMon**

#### IP Header

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_tos</td>
<td>Type Of Service field</td>
<td><code>ip_tos=1</code></td>
</tr>
<tr>
<td>ip_len</td>
<td>Total Length field</td>
<td><code>ip_len=20</code></td>
</tr>
<tr>
<td>ip_id</td>
<td>Identification field</td>
<td><code>ip_id=100</code></td>
</tr>
<tr>
<td>ip_off</td>
<td>Flags and Fragment Offset fields</td>
<td><code>ip_off&gt;0</code></td>
</tr>
<tr>
<td>ip_ttl</td>
<td>TTL field</td>
<td><code>ip_ttl&lt;80</code></td>
</tr>
<tr>
<td>ip_p</td>
<td>Protocol field</td>
<td><code>ip_p=6</code></td>
</tr>
<tr>
<td>ip_sum</td>
<td>Header Checksum field</td>
<td><code>ip_sum!=0</code></td>
</tr>
<tr>
<td>src</td>
<td>Source address field</td>
<td><code>src=194.29.35.43</code></td>
</tr>
<tr>
<td>dst</td>
<td>Destination address field</td>
<td><code>dst=194.29.35.43</code></td>
</tr>
</tbody>
</table>

#### TCP

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>sport</td>
<td>Source port</td>
<td><code>sport=21</code></td>
</tr>
<tr>
<td>dport</td>
<td>Destination port</td>
<td><code>dport=21</code></td>
</tr>
<tr>
<td>th_seq</td>
<td>Sequence Number</td>
<td><code>th_seq=0</code></td>
</tr>
<tr>
<td>th_ack</td>
<td>Acknowledgment Number</td>
<td><code>th_ack&gt;0</code></td>
</tr>
<tr>
<td>th_flags</td>
<td>Control Bits</td>
<td><code>th_flags=TH_RST</code></td>
</tr>
<tr>
<td>th_win</td>
<td>Window</td>
<td><code>th_win&gt;128</code></td>
</tr>
<tr>
<td>th_sum</td>
<td>Checksum</td>
<td><code>th_sum!=0</code></td>
</tr>
<tr>
<td>th_upr</td>
<td>Urgent Pointer</td>
<td><code>th_upr!=0</code></td>
</tr>
<tr>
<td>syn</td>
<td>SYN flag is set</td>
<td><code>syn</code></td>
</tr>
<tr>
<td>fin</td>
<td>FIN flag is set</td>
<td><code>fin</code></td>
</tr>
</tbody>
</table>
### Macro

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>rst</td>
<td>RST flag is set</td>
<td>rst</td>
</tr>
<tr>
<td>ack</td>
<td>ACK flag is set</td>
<td>ack</td>
</tr>
<tr>
<td>first</td>
<td>First TCP packet (only SYN is set)</td>
<td>first</td>
</tr>
<tr>
<td>established</td>
<td>TCP handshake completed</td>
<td>established</td>
</tr>
<tr>
<td>not_first</td>
<td>Not first packet (SYN flag is not set)</td>
<td>not_first</td>
</tr>
<tr>
<td>last</td>
<td>Last TCP packet</td>
<td>last</td>
</tr>
<tr>
<td>tcpdone</td>
<td>FIN or RST flags are set</td>
<td>tcpdone</td>
</tr>
</tbody>
</table>

### UDP

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>sport</td>
<td>Source port</td>
<td>sport=21</td>
</tr>
<tr>
<td>dport</td>
<td>Destination port</td>
<td>dport=21</td>
</tr>
<tr>
<td>uh_ulen</td>
<td>length</td>
<td>uh_ulen&gt;100</td>
</tr>
<tr>
<td>uh_sum</td>
<td>Checksum</td>
<td>uh_sum=0</td>
</tr>
</tbody>
</table>

### ICMP

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp_type</td>
<td>Type</td>
<td>icmp_type=ICMP_ECHOREPLY</td>
</tr>
<tr>
<td>icmp_code</td>
<td>Code</td>
<td>icmp_code=ICMP_UNREACH_NET</td>
</tr>
<tr>
<td>icmp_cksum</td>
<td>Checksum</td>
<td>icmp_cksum=0</td>
</tr>
</tbody>
</table>

### Useful INSPECT macros supported by PacketMon

#### Accept Specified Protocol Only

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>Accept only TCP protocol</td>
<td>tcp</td>
</tr>
<tr>
<td>udp</td>
<td>Accept only UDP protocol</td>
<td>udp</td>
</tr>
<tr>
<td>icmp</td>
<td>Accept only ICMP protocol</td>
<td>icmp</td>
</tr>
</tbody>
</table>

#### Accept packets to or from a host or port

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Accept only from given source or destination IP address</td>
<td>host(91.90.128.4)</td>
</tr>
</tbody>
</table>
**Monitoring and Troubleshooting**

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcpport</td>
<td>Accept only TCP packets with given source or destination port number</td>
<td>tcpport(21)</td>
</tr>
<tr>
<td>udpport</td>
<td>Accept only UDP packets with given source or destination port number</td>
<td>udpport(500)</td>
</tr>
<tr>
<td>port</td>
<td>Accept only TCP or UDP packets with given source or destination port number</td>
<td>port(300)</td>
</tr>
</tbody>
</table>

**Accept packets to or from computers on a specified network**

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>from_net</td>
<td>Accept only packets coming from the given network (source IP)</td>
<td>from_net(91.90.0.0,16)</td>
</tr>
<tr>
<td>to_net</td>
<td>Accept only packets sent to the given network (destination IP)</td>
<td>to_net(91.90.128.0,24)</td>
</tr>
<tr>
<td>net</td>
<td>Accept only packets coming from or going to the given network</td>
<td>net(194.29.35.0,24)</td>
</tr>
</tbody>
</table>

**Accept specified ICMP types**

<table>
<thead>
<tr>
<th>Macro</th>
<th>Purpose</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp_error</td>
<td>Accept ICMP errors</td>
<td>icmp_error</td>
</tr>
<tr>
<td>echo_req</td>
<td>Accept only ICMP echo requests</td>
<td>echo_req</td>
</tr>
<tr>
<td>echo_reply</td>
<td>Accept only ICMP echo replies</td>
<td>echo_reply</td>
</tr>
<tr>
<td>ping</td>
<td>Accept only ICMP echo requests and replies</td>
<td>ping</td>
</tr>
</tbody>
</table>

**Troubleshooting SCV**

"file is corrupt"

**Symptom**  
Client shows an error message: Compliance Policy file is corrupt. Please contact your system administrator.

**Scenario**  
An SCV check defined in the **SCVPolicy** section is not defined in the **local.scv** policy, **SCVNames** section.

**Solution**  
Make sure that the SCVNames section includes all the checks that are to be run on clients.
"unsupported format"

**Symptom**  
Client shows an error message: Compliance Policy is in an supported format

**Scenario**  
Can be one of these issues:

- There is no **SCVObject** section in the **local.scv** policy file.
- An SCV plug-in configured in the **local.scv** policy file does not exist on the client computer, or it has a functionality issue.
- The SCV Check type as defined in the local.scv policy is not a plug-in.
- The **local.scv** policy context has an incorrect format.
- The **local.scv** file was edited on an operating system that is different than the gateway operating system and the file was saved in an encoding that the gateway cannot read.

**Solution**  
See the SCV section in this Administration Guide and follow the instructions to edit and maintain the **local.scv** file.

"policy is not updated"

**Symptom**  
Client shows an error message: Compliance policy is corrupt. Please connect again to update the policy.

**Scenario**  
The policy enforced on the client computer is not updated with the latest security policy defined on the gateway.

**Solution**  
Connect the client computer again to the gateway. The client pulls the latest security policy when it connects to the gateway.

**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**

To enable Implicit MEP, you must install the Hotfix on the Security Management Server and on each Security Gateway. For Manual MEP this is not necessary.

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.
Advanced Configurations

In This Section:
Overlapping Encryption Domains .............................................................................. 116

Overlapping Encryption Domains

Overlapping encryption domains within a single site are supported for Remote Access Clients based on the specifications described below. A gateway’s encryption domain includes all IP addresses behind the gateway. This is based on the topology configured for the gateway. Alternatively, you can set a different domain for the Remote Access Community from the Topology page of the Gateway Properties.

Full Overlap

In the figure below, the encryption domains of Gateway A and Gateway B fully overlap - this means that they are identical.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote Access Client</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Gateway A</td>
</tr>
<tr>
<td>3E</td>
<td>Encryption Domain for Gateway A</td>
</tr>
<tr>
<td>4</td>
<td>Gateway B</td>
</tr>
<tr>
<td>4E</td>
<td>Encryption Domain for Gateway B</td>
</tr>
</tbody>
</table>

When the client attempts to create an encrypted connection with one of the hosts in the encryption domain, it chooses a gateway based on the configured MEP settings.
If the MEP setting is **First-to-respond** (the default), the client tries to connect to both gateways. The encrypted connection is created with the first gateway that responds.

If the MEP setting is **Load Distribution**, the client randomly selects a gateway.

### Partial Overlap

When there is a partial overlap between the encryption domains, there is at least one host that is in the encryption domain of two gateways. The other hosts are not in both encryption domains. For example, in the picture below, there is one host that is in the encryption domains of Gateway A and Gateway B. The other hosts are only in one encryption domain. Remote Access Clients do not support partially overlapping encryption domains.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote Access Client</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Gateway A</td>
</tr>
<tr>
<td>3E</td>
<td>Encryption Domain for Gateway A</td>
</tr>
<tr>
<td>4</td>
<td>Gateway B</td>
</tr>
<tr>
<td>4E</td>
<td>Encryption Domain for Gateway B</td>
</tr>
</tbody>
</table>

### Proper Subset

When:

- The encryption domain of Gateway B is fully contained in the encryption domain of Gateway A,
- But Gateway A also has additional hosts that are not in Gateway B,

Then Gateway B is a proper subset of Gateway A.
For example, in the picture below, Gateway B is a proper subset of Gateway A.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote Access Client</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Gateway A</td>
</tr>
<tr>
<td>3E</td>
<td>Encryption Domain for Gateway A</td>
</tr>
<tr>
<td>4</td>
<td>Gateway B</td>
</tr>
<tr>
<td>4E</td>
<td>Encryption Domain for Gateway B</td>
</tr>
</tbody>
</table>

Remote Access Clients support overlapping encryption domains of this type using Secondary Connect. The client creates an encrypted connection with the gateway closest to the host (the innermost gateway). In the picture above, the client creates an encrypted connection with Gateway B for hosts in Gateway B’s encryption domain, and with Gateway A for all other hosts.
In the figure below, three encrypted domains are nested inside each other.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote Access Client</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Gateway A</td>
</tr>
<tr>
<td>3E</td>
<td>Encryption Domain for Gateway A</td>
</tr>
<tr>
<td>4</td>
<td>Gateway B</td>
</tr>
<tr>
<td>4E</td>
<td>Encryption Domain for Gateway B</td>
</tr>
<tr>
<td>5</td>
<td>Gateway C</td>
</tr>
<tr>
<td>5E</td>
<td>Encryption Domain for Gateway C</td>
</tr>
</tbody>
</table>

The client creates encrypted connections according to these rules:

<table>
<thead>
<tr>
<th>Host</th>
<th>Connects to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts in Gateway C’s encryption domain</td>
<td>Gateway C</td>
</tr>
<tr>
<td>Host only in gateway B’s encryption domain and not in another encryption domain</td>
<td>Gateway B</td>
</tr>
<tr>
<td>All other hosts</td>
<td>Gateway A</td>
</tr>
</tbody>
</table>
**Backup Gateways**

**No Overlapping Encryption Domains**

The picture below shows two geographically separated internal networks that are connected to each other with a dedicated link. Each network is connected to the Internet through its own gateway. The encryption domains of Gateway A and Gateway B do not overlap, but Gateway B is defined as a backup for Gateway A.

![Diagram of two geographically separated internal networks connected by a dedicated link, with each network connected to the Internet through its own gateway. Gateway B is defined as a backup for Gateway A.]

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote Access Client</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Gateway A</td>
</tr>
<tr>
<td>3E</td>
<td>Encryption Domain for Gateway A</td>
</tr>
<tr>
<td>3N</td>
<td>Internal Network for Gateway A</td>
</tr>
<tr>
<td>4</td>
<td>Gateway B</td>
</tr>
<tr>
<td>4E</td>
<td>Encryption Domain for Gateway B</td>
</tr>
<tr>
<td>4N</td>
<td>Internal Network for Gateway B</td>
</tr>
<tr>
<td>5</td>
<td>Dedicated Link</td>
</tr>
</tbody>
</table>

When the client tries to establish a connection with one of the hosts in Gateway A’s encryption domain, it first tries to connect to Gateway A. If Gateway A is not available, it tries to connect through Gateway B.
**Fully Overlapping Encryption Domains**

Like the previous picture, the picture below shows two geographically separated internal networks that are connected to each other with a dedicated link. But in the picture below, Gateways A and B have identical encryption domains. Gateway C is in a different geographic location and is defined as a backup gateway for Gateways A and B.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remote Access Client</td>
</tr>
<tr>
<td>2</td>
<td>Internet</td>
</tr>
<tr>
<td>3</td>
<td>Gateway A</td>
</tr>
<tr>
<td>3E</td>
<td>Encryption Domain for Gateway A</td>
</tr>
<tr>
<td>4</td>
<td>Gateway B</td>
</tr>
<tr>
<td>4E</td>
<td>Encryption Domain for Gateway B</td>
</tr>
<tr>
<td>5</td>
<td>Gateway C</td>
</tr>
<tr>
<td>5E</td>
<td>Encryption Domain for Gateway C</td>
</tr>
<tr>
<td>6</td>
<td>Dedicated Link</td>
</tr>
</tbody>
</table>

When the client tries to establish a connection with one of the hosts in the encryption domain, it first tries to connect to the primary gateway based on the MEP settings configured (Gateways A and B in the example). It creates the encrypted connection with the first gateway that replies. If the primary gateways do not respond, the client tries to connect through Gateway C.
Remote Access Clients Command Line

In This Appendix

Using the Command Line ........................................................................................................122
CLI Commands .....................................................................................................................122

Using the Command Line

Remote Access Clients can be run from the command line. The basic syntax is trac <command>[<args>].

To use the command line:

1. Open a terminal: Start > Run > cmd

   Note - If you are using Windows 7 (or above) User Account Control (UAC), right-click the cmd.exe icon and select Run as Administrator.

2. Browse to the Remote Access Clients directory:
   - 32-bit system - C:\Program Files\CheckPoint\Endpoint Connect\trac
   - 64-bit system - C:\Program Files (x86)\CheckPoint\Endpoint Connect\trac

3. Run: trac <command> <arg>.

CLI Commands

These commands can be used for Remote Access Clients.

change_p12_pwd

<table>
<thead>
<tr>
<th>change_p12_pwd</th>
</tr>
</thead>
</table>

Description: Changes the password of a p12 certificate.

Syntax: trac change_p12_pwd -f <filename> [-o <old password> -n <new password>]

Arguments

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>name of the site</td>
</tr>
<tr>
<td>-f</td>
<td>pathname to the certificate file</td>
</tr>
<tr>
<td>-o</td>
<td>old password for the certificate</td>
</tr>
<tr>
<td>-n</td>
<td>new password for the certificate</td>
</tr>
</tbody>
</table>
change_p12_pwd

Example

trac change_p12_pwd -f "d:\My Documents\certs\mycert.p12" -o mypass -n sTr0ng3r_p1110Rd

You can use the feature interactively:

trac change_p12_pwd -f C:\myfile.p12
enter old password:****
enter new password:****
reenter new password:****

connect

Description
Connects the local client to a site.

Syntax
trac connect [\-s <site>] [\-g <gateway>] [\-u <user> \-p <password>] | \-d <dn> | \-f <p12> | \-pin <PIN> \-sn <serial>]

Arguments

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
</table>
| \-s  | Name of the site  
If not given, the client connects to the active site.  
If no active site is defined, an error message is given. |
| \-g  | Name of the gateway of this site.  
If not given, the client connects to the preferred gateway.  
If the client is already connected, this can be used to connect a secondary tunnel. |
| \-u and \-p | username and password credentials |
| \-d  | DN |
| \-f and \-p | path name and password of P12 certificate file |
| \-pin and \-sn | SecurID PIN and passcode |

Example

- username and password:
  trac connect \-s 192.0.2.12 \-u aa \-p aaaa
- SecurId:
  trac connect \-s 192.0.2.12 \-u aa \-pin 1111 \-sn 1234
- p12 Certificate:
  trac connect \-s 192.0.2.12 \-f "C:\john.p12" \-p 1234
- capi certificate:
  trac connect \-s 192.0.2.12 \-d CN=john,OU=users,O=cpmodule..p86dj5

Note - If more than one certificate with the same DN is in your certificate store, add the serial number to the command to make sure the correct certificate is used. For example, CN=john,OU=users,O=cpmodule..p86dj5(SerialNum=41014)
connectgui

**connectgui**

**Description**  Connects to the gateway using the GUI. The GUI must be running. If a user’s authentication credentials are not cached, it opens the login page so the user can authenticate. If the name of the site is not entered, the client connects to the active site.

**Syntax**  
```
trac connectgui [-s <site name>]
```

**Arguments**  
[-s <site name>]  - name of the site to connect to

create

**create**

**Description**  Creates a new site and defines its authentication method.

**Syntax**  
```
trac create [-s <site> [-a <auth method>]]
```

**Arguments**  

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>name of the site</td>
</tr>
</tbody>
</table>
| -a   | Valid values:  
  - username-password  
  - certificate  
  - p12-certificate  
  - challenge-response  
  - securIDKeyFob  
  - securIDPinPad  
  - SoftID |

**Example**
```
trac create -s mygateway.domain.com
trac create -s mygateway.domain.com -a certificate
```

delete

**delete**

**Description**  Deletes a site definition.

**Syntax**  
```
trac delete -s <site>
```

**Arguments**  

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>name of the site</td>
</tr>
</tbody>
</table>
### delete

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>trac delete -s mygateway.domain.com</td>
</tr>
</tbody>
</table>

### disable_log

**disable_log**

**Description**: Stops logging.

**Syntax**: trac disable_log

**Arguments**: none

### disconnect

**disconnect**

**Description**: Disconnects the local client from the current connection.

**Syntax**: trac disconnect [-g <gateway>]

**Arguments**:

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
</table>
| -g   | Name of gateway to disconnect.  
      | Optional parameter that can be used to disconnect a specified tunnel.  
      | If not given, the client disconnects the active site. |

### enable_log

**enable_log**

**Description**: Enables logging.

**Syntax**: trac enable_log

**Arguments**: none

### enroll_capi

**enroll_capi**

**Description**: Enrolls a CAPI certificate.
enroll_capi

Syntax

trac enroll_capi -s <site> -r <key> [-i <providerindex> -l <keylength> -sp <strongkeyprotection>]

Arguments

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>name or IP address of the site</td>
</tr>
<tr>
<td>-r</td>
<td>registration key</td>
</tr>
</tbody>
</table>
| -i   | where to store the certificate  
If you do not enter this in the command, the output shows the options. |
| -l   | length of the registration key |
| -sp  | whether strong key protection is used  
Valid values: “true” or “false” |

Example

trac enroll_capi -s mygateway.domain.com -r 654321
providers:
0. Gemplus GemSAFE Card CSP v1.0
1. Infineon SICRYPT Base Smart Card CSP
2. Microsoft Base Cryptographic Provider v1.0
3. Microsoft Enhanced Cryptographic Provider v1.0
4. Microsoft Strong Cryptographic Provider
5. Schlumberger Cryptographic Service Provider

enroll_p12

Description

Enrolls a p12 certificate.

Syntax

trac enroll_p12 -s <site> -f <filename> -p <password> -r <key> [-l <keylength>]

Arguments

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>name of the site</td>
</tr>
<tr>
<td>-f</td>
<td>pathname to the certificate file</td>
</tr>
<tr>
<td>-p</td>
<td>password for the certificate</td>
</tr>
<tr>
<td>-r</td>
<td>registration key</td>
</tr>
<tr>
<td>-l</td>
<td>length of the key</td>
</tr>
</tbody>
</table>

Example

trac enroll_p12 -s mygateway.domain.com -f "d:\My Documents\certs\mycert.p12" -p mypass -r 654321
**firewall**

**Description**  Enables or disables the Desktop firewall

**Syntax**  
```
firewall -st enable|disable
```

**Arguments**  None

**help**

**Description**  Outputs help on the CLI or for a command.

**Syntax**  
```
trac help | h
```

**Arguments**  None, but if a command is given, help for that command is shown

**hotspot_reg**

**Description**  Temporarily allows endpoint connections from Hotspots in public places, such as airports and hotels, so that the user can register with the Hotspot portal.

**Syntax**  
```
hotspot_reg
```

**Arguments**  None

⚠️ **Important** - Make sure that the Security Management Server is configured to enable any port for HotSpot registration.

**info**

**Description**  Outputs all sites configured and their gateways, including current tunnel status.

**Syntax**  
```
trac info [-s <site name>]
```
## info

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-s`      | name of the site  
If given, only gateways and tunnel information for this site are shown. |

### Example
```
trac info  
trac info -s mygateway.domain.com
```

## List

### Description
Shows certificate subject names stored in the CAPI.

### Syntax
```
trac List
```

### Arguments
none

### Example
```
C:\Program Files\CheckPoint\Endpoint Connect>trac list  
User's DNs:  
CN=John,OU=users,O=cpmodule..p86dj5(SerialNum=41014)  
C:\Program Files\CheckPoint\Endpoint Connect>
```

## Log

### Description
Shows messages for "no network" and "service is down".

### Syntax
```
trac Log
```

### Arguments
none

### Example
```
C:\Program Files\CheckPoint\Endpoint Connect>trac log  
Waiting for log events...  
***** Accepted network event: no network  
***** Accepted network event: client is in an insecure environment  
***** Accepted Stop event - Endpoint Security service is down
```

## renew_capi

### Description
Renews a capi certificate.

### Syntax
```
trac renew_capi -s <sitename> -d <dn> [ -l <keylength> -sp <strongkeyprotection> ]
```
### renew_capi

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td></td>
<td>name of the site</td>
</tr>
<tr>
<td>-d</td>
<td></td>
<td>certificate subject name</td>
</tr>
<tr>
<td>-l</td>
<td></td>
<td>length of the registration key</td>
</tr>
<tr>
<td>-sp</td>
<td></td>
<td>if strong key protection is used (Valid values: &quot;true&quot; or &quot;false&quot;)</td>
</tr>
</tbody>
</table>

**Example**

```
trac renew_capi -s 192.0.2.0
   -d CN=yCert,OU=users,O=cpmodule..p86dj5
```

### renew_p12

#### Description

Renews a p12 certificate.

#### Syntax

```
trac renew_p12 -s <site> -f <filename> -p <password> [-l <keylength>]
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td></td>
<td>name of the site</td>
</tr>
<tr>
<td>-f</td>
<td></td>
<td>pathname for the certificate file</td>
</tr>
<tr>
<td>-p</td>
<td></td>
<td>password for the certificate</td>
</tr>
<tr>
<td>-l</td>
<td></td>
<td>length of the key</td>
</tr>
</tbody>
</table>

**Example**

```
trac renew_p12 -s mygateway.domain.com -f "<full path> mycert.p12" -p mypass
```

### set_proxy_settings

#### Description

```
trac set_proxy_settings [-m <mode>] [-h <hostname> -po <port> ] [-u <username> -p <password>]
```
Arguments

<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m mode</td>
<td>one of no_proxy</td>
</tr>
<tr>
<td></td>
<td>• no_proxy - To disable proxy setting</td>
</tr>
<tr>
<td></td>
<td>• auto - To take proxy settings from the Internet</td>
</tr>
<tr>
<td></td>
<td>• manual - To set the proxy address (i.e. hostname and port)</td>
</tr>
<tr>
<td>-h</td>
<td>hostname and port of the proxy</td>
</tr>
<tr>
<td>-p</td>
<td>This can be set only when the proxy mode is manual</td>
</tr>
<tr>
<td>-u</td>
<td>username and password credentials</td>
</tr>
<tr>
<td>-p</td>
<td>This can be set only when the proxy mode is not no_proxy</td>
</tr>
</tbody>
</table>

Example

```
trac set_proxy_settings -m manual -h 192.168.1.1 -po 12345 -u user -p pass
```

start

Description
Starts the Remote Access Clients service.

Syntax
```
trac start
```

Arguments
none

Note - If User Account Control is enabled, this command requires administrative privileges.

stop

Description
Stops the Remote Access Clients service.

Syntax
```
trac stop
```

Arguments
none

Note - If User Account Control is enabled, this command requires administrative privileges.

Ver

Description
Shows the version of the client.

Syntax
```
trac Ver
```
Ver

Arguments  none

sdl

Description  Enable or disable Secure Domain Logon (SDL).
Syntax  trac sdl -st <state>
Arguments  
<table>
<thead>
<tr>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-st</td>
<td>SDL state – “enable” / “disable”</td>
</tr>
</tbody>
</table>
Example  trac sdl -st enable
         trac sdl -st disable

userpass

Description  For ATM clients, sets the username and password.
Syntax  trac userpass -s <sitename> -u <username> -p <password>
Example  To set username and password:
         trac userpass -s <sitename> -u <username> -p <password>
         To delete username and password:
         userpass -s <sitename>

certpass

Description  For ATM clients, sets the certificate path and password.
Syntax  trac certpass -s <sitename> -f <certificate filename> -p <password>
Example  To set username and password:
         trac certpass -s <sitename> -f <certificate filename> -p <password>
         To delete certificate credentials:
         certpass -s <sitename>
Creating a DLL file to use with SAA

In This Appendix

OPSEC - Open Platform for Security ................................................................. 132
Overview of SAA ......................................................................................... 132
How Does SAA Work ................................................................................ 132
Summary of OPSEC API Functions............................................................. 133

OPSEC - Open Platform for Security

Check Point’s OPSEC (Open Platform for Security) integrates and manages all of network security through an open, extensible management framework. Third party security applications can plug into the OPSEC framework via published application programming interfaces (APIs). Once integrated into the OPSEC framework, applications can be configured and managed from a central point, utilizing a single Security Policy editor. This document describes the OPSEC Secure Authentication API (SAA), which enables third-party authentication technologies to be used with Check Point Clients.

Overview of SAA

This section describes the technical requirements for a DLL file to use with Secure Authentication API (SAA). Secure Authentication API (SAA) lets you use third-party authentication technologies with Remote Access Clients. When you configure SAA for a site, users authenticate to the site with an authentication scheme specific to your organization. For example, if your organization uses biometric authentication, users can use the same biometric authentication to authenticate to the site.

The DLL acts as the authentication agent and defines how the client gets the Third Party authentication information and what it does with the information. The file must implement and export the OPSEC API Functions listed in the next sections.

How Does SAA Work

Check Point clients are located between the computer’s network adapter and TCP/IP stack. This lets the client intercept all packets entering or leaving the computer and to encrypt or decrypt them as necessary.

Scenario with a non-SAA Authentication Method

This scenario describes an example of what happens when a user, Hugo, connects to a site on the London gateway with a non-SAA authentication method.

1. Hugo initiates a connection to a host in the London gateway’s encryption domain.
2. The Check Point client sends Hugo’s username to the Security Management Server that also manages the Check Point clients.
3. The Security Management Server challenges Hugo to authenticate himself according to the authentication scheme configured for that site.

4. Hugo enters the response to the challenge (usually a password).

5. If the response was correct, the Check Point client and the Security Management Server exchange a session key. This key is used to encrypt the data connection.

Scenario with SAA

This scenario describes an example of what happens when a user, Hugo, connects to a site on the London gateway with SAA Authentication. The Check Point client acts as a proxy for a third party Authentication Agent.

1. The Authentication Agent exports a small number of functions in an Authentication DLL file (located on the user’s machine).

2. These functions let the client forward the Security Management server’s challenges to the Authentication Agent on Hugo’s machine.

3. The client forwards the responses from the Authentication Agent back to the Security Management Server.

4. When Hugo initiates a connection to a host in the London gateway’s encryption domain the Check Point client calls the appropriate functions in the Authentication DLL rather than displaying the standard login windows.

5. When the Security Management Server decides to accept or deny the connection, a status indicator is sent to the Authentication Agent.

6. The Check Point client and the Security Management Server exchange a session key. This key is used to encrypt the data connection.

   Note - The SAA DLL is only responsible for providing the username and the correct responses to the Security Management server’s challenges. The actual key exchange is still done by the Check Point client.

Important Note on Working with SAA

In this version of Remote Access Clients the SAA DLL cannot determine which site a user is authenticating to. Therefore the client might give the authentication credentials supplied by the Authentication Agent to the wrong site. The authentication will probably fail, but the wrong site will have the user’s credentials.

When you create the DLL file, try to prevent the wrong site from accidentally receiving private information. For example, the Authentication Agent can display the site name, as provided by the username function, to let users and Authentication Agent distinguish between different sites.

Summary of OPSEC API Functions

We recommend that you use Version 2 API. If you have legacy clients that use Version 1, include Version 1 API functions for backward compatibility.

To understand the advantages of Version 2, see the legacy Secure Authentication API Specification [http://downloads.checkpoint.com/dc/download.htm?ID=7389].
**Note** - The function prototypes are defined in the file `authplugin.h` which can be found on the OPSEC Desktop SDK [http://downloads.checkpoint.com/dc/download.htm?ID=7390].

<table>
<thead>
<tr>
<th>API Function</th>
<th>Version (Ver)</th>
<th>Summary of Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>PickVersion</td>
<td>Optional for Ver 1. Required for Ver 2</td>
<td>Supplies the lower and higher API versions that the client supports. From these versions, the Authentication Agent chooses which it prefers, and the client uses that selection. If PickVersion is not in the DLL, the Client assumes you are using Version1.</td>
</tr>
<tr>
<td>RegisterAgent or</td>
<td>RegisterAgent - Ver 1 RegisterAgentVer2 - Ver 2</td>
<td>Supplies the client with the functions required to work with the Authentication Agent.</td>
</tr>
<tr>
<td>RegisterAgentVer2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>For Ver 1 and Ver 2</td>
<td>Supplies the username to be used by the client to authenticate with the gateway for SAA Challenge/Response authentication.</td>
</tr>
<tr>
<td>UserNameAndPassword or</td>
<td>UserNameAndPassword - Ver 1 UserNameAndPasswordVer2 - Ver 2</td>
<td>Supplies the username and password to be used by the client to authenticate with the gateway for SAA Username/Password authentication.</td>
</tr>
<tr>
<td>UserNameAndPasswordVer2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response</td>
<td>For Ver 1 and Ver 2</td>
<td>The client gives the Authentication Agent the challenge that it gets from the gateway. The Authentication Agent returns a response that the client sends back to the gateway.</td>
</tr>
<tr>
<td>AuthCompleted or Terminate</td>
<td>Terminate - Ver 1 AuthCompleted - Ver 2</td>
<td>The client tells the Authentication Agent when authentication has completed and its result. The Authentication Agent can notify the user of the authentication’s results.</td>
</tr>
<tr>
<td>ReleaseContext</td>
<td>Only for Ver 2</td>
<td>Is called when the client wants to delete context, for example, when a password is expired or has been erased.</td>
</tr>
<tr>
<td>VendorDescription</td>
<td>For Ver 1 and Ver 2</td>
<td>Returns a meaningful name that the client can display to the user.</td>
</tr>
<tr>
<td>GoingDown</td>
<td>For Ver 1 and Ver 2</td>
<td>Is called when the client session is going to terminate.</td>
</tr>
</tbody>
</table>
### API Function

<table>
<thead>
<tr>
<th>API Function</th>
<th>Version (Ver)</th>
<th>Summary of Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>InvalidateProcCB</td>
<td>For Ver 1 and Ver 2</td>
<td>Instructs the client to invalidate previous authentications.</td>
</tr>
</tbody>
</table>

### PickVersion

PickVersion supplies the lower and higher API versions that the client supports. From these versions, the Authentication Agent chooses which it prefers, and the client uses that selection. If PickVersion is not in the DLL, the Authentication Agent assumes you are using Version 1.

**Prototype**

```c
int PickVersion(int minVersion, int maxVersion)
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>minVersion</td>
<td>In</td>
<td>Minimum supported client version</td>
</tr>
<tr>
<td>maxVersion</td>
<td>In</td>
<td>Maximum supported client version</td>
</tr>
</tbody>
</table>

**Return Values**

The version number that the Authentication Agent wants to use.

A return value that is lower than `minVersion` or higher than `maxVersion` is **not supported**.

### RegisterAgent or RegisterAgentVer2

RegisterAgent for Version 1 or RegisterAgentVer2 for Version 2 supply the client with the functions required to work with the Authentication Agent.

### RegisterAgentVer2

**Prototype**

```c
int RegisterAgentVer2(int* version,
                      UserNameProcType* usernameProc,
                      UserNameAndPasswordVer2ProcType* usernameAndPasswordVer2Proc,
                      ResponseProcType* responseProc,
                      GoingDownProcType* goingdownProc,
                      AuthCompletedProcType* authCompletedProc,
                      ReleaseContextProcType* releaseContextProc,
                      InvalidateProcType invalidateProcCB)
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>In</td>
<td>The version number of the API supported by the client is 2.</td>
</tr>
<tr>
<td></td>
<td>Out</td>
<td>The version number of the API supported by the Authentication Agent is 2.</td>
</tr>
</tbody>
</table>
Creating a DLL file to use with SAA

Remote Access Clients for Windows 32/64-bit Administration Guide E80.71   |   136

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernameProc</td>
<td>Out</td>
<td>The address of the Authentication Agent’s UserName function.</td>
</tr>
<tr>
<td>usernameAndPasswordVer2Proc</td>
<td>Out</td>
<td>The address of the Authentication Agent’s UserNameAndPasswordVer2 function.</td>
</tr>
<tr>
<td>responseProc</td>
<td>Out</td>
<td>The address of the Authentication Agent’s Response function.</td>
</tr>
<tr>
<td>goingdownProc</td>
<td>Out</td>
<td>The address of the Authentication Agent’s GoingDown function.</td>
</tr>
<tr>
<td>authCompletedProc</td>
<td>Out</td>
<td>The address of the Authentication Agent’s AuthCompleted function.</td>
</tr>
<tr>
<td>releaseContextProc</td>
<td>Out</td>
<td>The address of the Authentication Agent’s ReleaseContext function.</td>
</tr>
<tr>
<td>invalidateProcCB</td>
<td>In</td>
<td>The address of the client callback function that invalidates previous authentication information. The Authentication Agent might call this function to force reauthentication.</td>
</tr>
</tbody>
</table>

Return Values

PLUGIN_OK if successful.

PLUGIN_ABORT if the specified version of the client is not supported.

**RegisterAgent**

Prototype

```c
int RegisterAgent( int *version,
UserNameProcType *Username,
UserNameAndPasswordProcType *usernameAndPassword,
ResponseProcType *Response,
TerminateProcType *Terminate,
GoingDownProcType *Goingdown,
InvalidateProcType InvalidateProcCB )
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>In</td>
<td>The version number of the API supported by the client is 1.</td>
</tr>
<tr>
<td></td>
<td>Out</td>
<td>The version number of the API supported by the Authentication Agent is 1.</td>
</tr>
<tr>
<td>Username</td>
<td>Out</td>
<td>The address of the Authentication Agent’s UserName function.</td>
</tr>
</tbody>
</table>
Creating a DLL file to use with SAA

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>usernameAndPassword</td>
<td>Out</td>
<td>The address of the Authentication Agent’s UserNameAndPassword function.</td>
</tr>
<tr>
<td>Response</td>
<td>Out</td>
<td>The address of the Authentication Agent’s Response function.</td>
</tr>
<tr>
<td>Terminate</td>
<td>Out</td>
<td>The address of the Authentication Agent’s Terminate function.</td>
</tr>
<tr>
<td>Goingdown</td>
<td>Out</td>
<td>The address of the Authentication Agent’s GoingDown function.</td>
</tr>
<tr>
<td>invalidateProcCB</td>
<td>In</td>
<td>The address of the client callback function that invalidates previous authentication information. The Authentication Agent might call this function to force reauthentication.</td>
</tr>
</tbody>
</table>

Return Values

- PLUGIN_OK if successful.
- PLUGIN_ABORT if the specified version of the client is not supported.

VendorDescription

For Version 1 and Version 2.

VendorDescription returns a meaningful name that the client can display to the user.

Prototype

```c
char *VendorDescription()
```

Arguments

There are no arguments.

Return Values

A static string defined in the Authentication DLL. The client does not make copies of the return value- it uses it directly.

UserName

For Version 1 and Version 2.

Username supplies the username to be used by the client to authenticate with the gateway for SAA Challenge/Response authentication.

If the Authentication Agent wants to handle the authentication, it must supply a username, and a [possibly NULL] context. If the Authentication Agent does not want to handle the authentication, it returns PLUGIN_ABORT. The authentication is then handled by the client.
Prototype

```c
int Username(char *site, char *username, int *usernameLength, void **context);
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>site</td>
<td>In</td>
<td>The name of the site being accessed, as defined in the client Sites window. This lets the Authentication Agent display the name of the site.</td>
</tr>
<tr>
<td>username</td>
<td>Out</td>
<td>The buffer to which username should be copied.</td>
</tr>
<tr>
<td>usernameLength</td>
<td>In</td>
<td>Length of the buffer allocated for username.</td>
</tr>
<tr>
<td></td>
<td>Out</td>
<td>If username is longer than the specified length, the function should return PLUGIN_DATA_TOO_LONG and use this argument to indicate the number of bytes required.</td>
</tr>
<tr>
<td>context</td>
<td>Out</td>
<td>A context supplied by the Authentication Agent to be used in subsequent calls to Response.</td>
</tr>
</tbody>
</table>

Return Values

- PLUGIN_OK if successful.
- PLUGIN_ABORT if the client should take over the authentication.
- PLUGIN_DATA_TOO_LONG if the buffer specified by username is not long enough.
- PLUGIN_CANCEL if the authentication should be terminated. This should be used with discretion since Authentication Agents generally do not have enough information to determine whether the authentication should be cancelled.

UsernameAndPassword or UserNameAndPasswordVer2

UsernameAndPassword for Version 1 or UserNameAndPasswordVer2 for Version 2 supplies the username to be used by the client to authenticate with the gateway for SAA Username/Password authentication.

If the Authentication Agent wants to handle the authentication, it must supply a username, password, and a context. If the Authentication Agent does not want to handle the authentication, it returns PLUGIN_ABORT. The authentication is then handled by the client.

UserNameAndPasswordVer2

Prototype

```c
UserNameAndPasswordVer2Proc(char* site, char* username, int* usernameLength, char* password, int* passwordLength, void** context);
```
Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>site</td>
<td>In</td>
<td>The name of the site being accessed, as defined in the client Sites window. This lets the Authentication Agent display the name of the site.</td>
</tr>
<tr>
<td>username</td>
<td>Out</td>
<td>The buffer to which username should be copied.</td>
</tr>
<tr>
<td>usernameLength</td>
<td>In/Out</td>
<td>In - Length of the buffer allocated for username. Out - If username is longer than the specified length, the function should return PLUGIN_DATA_TOO_LONG and use this argument to indicate the number of bytes required.</td>
</tr>
<tr>
<td>password</td>
<td>Out</td>
<td>The buffer to which the password should be copied.</td>
</tr>
<tr>
<td>passwordLength</td>
<td>In/Out</td>
<td>In - Length of the buffer allocated for password. Out - If password is longer than the specified length, the function should return PLUGIN_DATA_TOO_LONG and use this argument to indicate the number of bytes required.</td>
</tr>
<tr>
<td>context</td>
<td>Out</td>
<td>A context supplied by the Authentication Agent to be used in subsequent calls to Response.</td>
</tr>
</tbody>
</table>

Return Values

PLUGIN_OK if successful.

PLUGIN_ABORT if the client should take over the authentication.

PLUGIN_DATA_TOO_LONG if the buffer specified by username and/or by password is not long enough.

PLUGIN_CANCEL if the authentication should be terminated. This should be used with discretion since Authentication Agents generally do not have enough information to determine whether the authentication should be cancelled.

UsernameAndPassword

Prototype

```c
int UserNameAndPassword(char *site, char *username, int *usernameLength, char *password, int *passwordLength);
```

Arguments

Same as UserNameAndPasswordVer2.
Return Values

Same as UserNameAndPasswordVer2.

Response

For Version 1 and Version 2.

The client gives the Authentication Agent the challenge that it gets from the gateway. The Authentication Agent shows the challenge to the user. The user enters a response to the challenge.

The Authentication Agent returns the user’s response back to the client, which forwards it to the gateway.

Prototype

```c
int Response( void *context, char *challenge, char *response,
int *responseLength);
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>context</td>
<td>In</td>
<td>The context as provided by Username</td>
</tr>
<tr>
<td>challenge</td>
<td>Out</td>
<td>The authentication challenge string as received from the Security Management Server.</td>
</tr>
<tr>
<td>response</td>
<td>Out</td>
<td>The buffer to which the Authentication Agent’s response is to be copied.</td>
</tr>
<tr>
<td>usernameLength</td>
<td>In,Out</td>
<td>In - Length of the buffer allocated for response.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Out - If username is longer than the specified length, the function should return PLUGIN_DATA_TOO_LONG and use this argument to indicate the number of bytes required.</td>
</tr>
</tbody>
</table>

Return Values

PLUGIN_OK if successful.

PLUGIN_ABORT if the client should take over the authentication.

PLUGIN_DATA_TOO_LONG if the buffer specified by response is not long enough.

PLUGIN_CANCEL if the authentication should be terminated. This should be used with discretion since Authentication Agents generally do not have enough information to determine whether the authentication should be cancelled.

Terminate

For Version 1.
The Client calls Terminate when authentication is complete or when a password has expired or been erased by the user. In response, the Authentication Agent might release allocated resources and notify the user of the results of the authentication.

**Prototype**

```c
int Terminate(void *context, int status, char *message);
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>context</td>
<td>In</td>
<td>The context as provided by Username or UsernameAndPassWord.</td>
</tr>
</tbody>
</table>
| status   | In     | The status of the authentication. One of these values:  
|          |        | • PLUGIN_DONE_SUCCESS - authentication was successful  
|          |        | • PLUGIN_DONE_FAILED - authentication failed  
|          |        | • PLUGIN_DONE - authentication has been cancelled for example, the password has expired or been erased. |
| message  | In     | The termination message, if provided by the authentication server. |

**Return Values**

PLUGIN_OK if successful.

PLUGIN_CANCEL if the input does not make sense.

---

**AuthCompleted**

For Version 2

The client calls AuthCompleted when authentication has completed. The Authentication Agent can notify the user of the authentication’s results.
**Argument** | **In/Out** | **Meaning**
--- | --- | ---
status | In | The status of the authentication. One of these values:
- PLUGIN_DONE_SUCCESS - authentication was successful
- PLUGIN_DONE_FAILED - authentication failed
- PLUGIN_DONE - authentication has been cancelled for example, the password has expired or been erased.
message | In | The termination message, if provided by the authentication server.

**Return Values**
- PLUGIN_OK if successful.
- PLUGIN_CANCEL if the input does not make sense.

**ReleaseContext**
For version 2.
ReleaseContext is called when the client wants to delete context, for example, when a password is expired or has been erased.

**Prototype**
```c
void ReleaseContext(void* context)
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>In/Out</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| context  | In     | The context as provided by `Username` or `UsernameAndPassWord`.

**Return Values**
None.

**GoingDown**
For Version 1 and Version 2
The client calls GoingDown when the client session is going to terminate.

**Prototype**
```c
void GoingDown()
```

**Arguments**
There are no arguments.

**Return Values**
None.
InvalidateProcCB

For Version 1 and Version 2

InvalidateProcCB tells the client to invalidate all previous authentications. The effect of calling InvalidateProcCB is the same as the effect of erasing passwords. It forces authentication for future connections, but does not terminate existing connections.

Prototype
void InvalidateProcCB()

Arguments
There are no arguments.

Return Values
None.