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.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=12320

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the home page (http://supportcontent.checkpoint.com/solutions?id=sk65209) at the Check Point Support Center.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 September 2011</td>
<td>First draft of this document.</td>
</tr>
</tbody>
</table>

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-bit/64-bit E75.20 Administration Guide).
## Contents

**Important Information** .......................................................................................3

**Introduction to Remote Access Clients** .............................................................7
   Endpoint Security VPN ......................................................................................7
   Check Point Mobile for Windows ....................................................................8
   SecuRemote .....................................................................................................8
   Features Overview ...........................................................................................8
   Connectivity Features in Detail .......................................................................9
   Security Features in Detail .............................................................................10
   Deployment Features .......................................................................................10
   General Features .............................................................................................11
   Topology Architecture .....................................................................................11
   Encryption Domains .......................................................................................11
   External Resources in Encryption Domain ....................................................12
   Related Documentation ...................................................................................12

**Setting Up Remote Access Clients** .................................................................14
   Installing the Remote Access Clients Hotfix ..................................................14
   Required Gateway Settings ............................................................................15
   Configuring a Policy Server ............................................................................18
   Remote Access Modes ....................................................................................19
   Endpoint Security VPN for Unattended Machines (ATMs) ............................19
   Automatic Upgrade from the Gateway ............................................................19
   Configuring Upgrades ....................................................................................20
   Distributing the Remote Access Clients from a package ..............................21
      Creating the Client Installation Package .....................................................21
      Authentication Schemes and Certificates ....................................................23
      Advanced Client Settings ..........................................................................29
   Editing an MSI Package with CLI .................................................................32
   Installing an MSI Package with CLI ..............................................................34
   Updating User Sites with the Update Configuration Tool..............................35
      Usage for Update Configuration Tool ..........................................................35
      Using the Update Configuration Tool .........................................................35

**Helping Your Users** .......................................................................................37
   Simple Installation ..........................................................................................37
   Remote Access Clients Client Icon ..............................................................37
   Helping Users Create a Site ............................................................................38
      Preparing the Gateway Fingerprint .............................................................38
      Using the Site Wizard .................................................................................38
      Opening the Site Wizard Again .................................................................39
   Helping Users with Basic Client Operations ................................................40

**Configuring Client Features** ..........................................................................41
   Installing Desktop Security Policy .................................................................41
   Managing Desktop Firewalls ..........................................................................41
      The Desktop Firewall ..................................................................................42
      Rules ...........................................................................................................42
      Default Policy .............................................................................................43
      Logs and Alerts ..........................................................................................43
   Wireless Hotspot/Hotel Registration ..............................................................43
   Planning Desktop Security Policy .................................................................44
   Operations on the Rule Base ..........................................................................44
   Making the Desktop Security Policy ..............................................................44
   Letting Users Disable the Firewall .................................................................45
   Secure Domain Logon (SDL) ..........................................................................45
Chapter 1

Introduction to Remote Access Clients

Remote Access Clients provide a simple and secure way for endpoints to connect remotely to corporate resources over the Internet, through a VPN tunnel. Check Point offers 3 enterprise-grade flavors of Remote Access to fit a wide variety of organizational needs.

The clients offered in this release are:

- **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.


In This Chapter

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security VPN</td>
<td>7</td>
</tr>
<tr>
<td>Check Point Mobile for Windows</td>
<td>8</td>
</tr>
<tr>
<td>SecuRemote</td>
<td>8</td>
</tr>
<tr>
<td>Features Overview</td>
<td>8</td>
</tr>
<tr>
<td>Topology Architecture</td>
<td>11</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>12</td>
</tr>
</tbody>
</table>

**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

- New 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.

Features 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>Proxy Detection</td>
<td>Proxy servers between the client and the gateway are automatically detected and authenticated to if necessary</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 tunnel test 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>
</tbody>
</table>
### Features Overview

<table>
<thead>
<tr>
<th>Main Capability</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 server 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 firewalls 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 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>Compliance Policy - Secure Configuration Verification (SCV)</td>
<td>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.</td>
</tr>
<tr>
<td>Secure Domain Logon (SDL)</td>
<td>Establishes a VPN tunnel before a user logs in.</td>
</tr>
</tbody>
</table>

### Connectivity Features in Detail

Remote Access Clients support more connectivity features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Connectivity Detection</td>
<td>If the IPSec VPN network connection is lost, the client seamlessly reconnects without user intervention.</td>
</tr>
<tr>
<td>Roaming</td>
<td>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.</td>
</tr>
<tr>
<td>Multiple Sites</td>
<td>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.</td>
</tr>
<tr>
<td>Dialup Support</td>
<td>Endpoint Security VPN supports dial-up connections, useful where a network is not detected.</td>
</tr>
<tr>
<td>Hotspot Detection and Registration</td>
<td>Automatically detects hotspots that prevent the client system from establishing a VPN tunnel. Opened a mini-browser to allow the user to register to the hotspot and connect to the VPN gateway.</td>
</tr>
<tr>
<td>Office Mode</td>
<td>Lets a remote client appear to the local network as if it is using a local IP address. This is not supported on SecuRemote.</td>
</tr>
<tr>
<td>Extended DHCP Parameters</td>
<td>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.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Machine Idleness</td>
<td>Disconnects the VPN tunnel if the machine becomes inactive (because of lock or sleep) for a specified duration.</td>
</tr>
<tr>
<td>Keep-alive</td>
<td>Send keep-alive messages from the client to the VPN gateway to maintain the VPN tunnel.</td>
</tr>
<tr>
<td>VPN Connectivity to VPN-1 VSX</td>
<td>Terminate VPN tunnel at Check Point VSX gateways.</td>
</tr>
<tr>
<td>Split DNS</td>
<td>Support multiple DNS servers.</td>
</tr>
<tr>
<td>DHCP Automatic Lease Renewal</td>
<td>Automatically renew IP addresses obtained from DHCP servers</td>
</tr>
</tbody>
</table>

### Security Features in Detail
Remote Access Clients support more security features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strong Authentication Schemes</strong></td>
<td></td>
</tr>
<tr>
<td>User names and passwords</td>
<td>Including cached passwords.</td>
</tr>
<tr>
<td>Challenge-Response</td>
<td>This is an authentication protocol in which one party provides the first string (the challenge), and the other party verifies it with the next string (the response). For authentication to take place, the response must be validated. Security systems that rely on SecurID are based on challenge-response.</td>
</tr>
<tr>
<td>CAPI software and hardware tokens</td>
<td>Cryptographic Application Program Interface enables access to a library of functions that provide security and encryption.</td>
</tr>
<tr>
<td>SecurID</td>
<td>Two-factor authentication. An example of a type of SecurID configuration requires a password and a token code. SecurID authentication methods supported by Remote Access Clients: Key Fob, PINPad, and Software Tokens.</td>
</tr>
<tr>
<td>Certificate Enrollment and Renewal</td>
<td>Enrollment refers to the process of application for, and receipt of, a certificate from a recognized Certificate Authority (CA), in this case Check Point's Internal CA. In the enrollment process, you create a certificate and send the registration key to users. The client sends this key to gateway, and in return receives the certificate. Renewal lets the client renew a certificate that is going to expire.</td>
</tr>
<tr>
<td>Tunnel Idleness Detection</td>
<td>Idle or inactive VPN tunnels are detected and shut down.</td>
</tr>
<tr>
<td>Smart Card Removal Detection</td>
<td>Detects when the Smart Card is removed and closes the active VPN tunnel.</td>
</tr>
<tr>
<td>Secure Authentication API (SAA)</td>
<td>Use third-party authentication technologies to authenticate to Remote Access Clients.</td>
</tr>
</tbody>
</table>

### Deployment Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Client Upgrade from the Gateway</td>
<td>Clients can automatically get an upgrade package when they connect to the gateway.</td>
</tr>
</tbody>
</table>
### General Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post Connect Scripts</td>
<td>Run a script on client computers after a connection to the gateway is established.</td>
</tr>
</tbody>
</table>

### 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

**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>
</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>
<tbody>
<tr>
<td>1 Gateway of Site 1</td>
<td>• Remote Access Clients , as their VPN gateway (5)</td>
</tr>
<tr>
<td></td>
<td>• External resource (4)</td>
</tr>
<tr>
<td></td>
<td>• Redirects clients (5) to external resource (4)</td>
</tr>
<tr>
<td>2 Remote Access Encryption Domain</td>
<td>Encrypted domain of gateway (1) that includes an external resource</td>
</tr>
<tr>
<td>3 Servers in Encryption Domain</td>
<td>External resource</td>
</tr>
<tr>
<td>4 External (Internet or DMZ) resource in</td>
<td>• Server in Encryption Domain</td>
</tr>
<tr>
<td>Encryption Domain</td>
<td>• Remote Access Clients if the gateway redirects</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>• External resource (4), through gateway redirect</td>
</tr>
</tbody>
</table>

### Related Documentation

Find all documents in sk65209 ([http://supportcontent.checkpoint.com/solutions?id=sk65209](http://supportcontent.checkpoint.com/solutions?id=sk65209)).

- Remote Access Clients E75.20 Release Notes
- Remote Access Clients E75.20 Administration Guide
- Endpoint Security VPN E75.20 User Guide
- Check Point Mobile for Windows E75.20 User Guide
- SecuRemote E75.20 User Guide

Environments with SecureClient already deployed can be easily upgraded to Endpoint Security VPN or Check Point Mobile for Windows. Clients who had SecuRemote client can use the same steps to upgrade to SecuRemote E75.20. The SmartDashboard for different versions of management servers is different. Use the documentation for the SmartDashboard that you have. All guides are in sk65209 (http://supportcontent.checkpoint.com/solutions?id=sk65209).

- For NGX R65 SmartCenter Server, NGX R65.70 or higher, see Remote Access Clients E75.20 Upgrade Guide from SecureClient/SecuRemote NGX on NGX R65.

- For R70 Security Management Server, R70.40 or higher, see Remote Access Clients E75.20 Upgrade Guide from SecureClient/SecuRemote NGX on R70.

- For R71 Security Management Server, R71.30 or higher, or R75 Security Management Server, see Remote Access Clients E75.20 Upgrade Guide from SecureClient/SecuRemote NGX on R71 or R75.
Chapter 2

Setting Up Remote Access Clients

Remote Access Clients requires a supported gateway version. If you use Automatic MEP, the Security Management Server or Multi-Domain Server must also be supported, with required hotfixes as needed.

See the Remote Access Clients E75.20 Release Notes to see if a hotfix is required for your environment.

The initial workflow includes:

- Install the gateway Hotfix, if required.
- Configure the gateway.
- Download one of the client packages from the Download Center (TRAC.cab or MSI).
- Edit the package and distribute it either:
  - Automatically on the gateway, using the TRAC.cab file. This is only for users who are upgrading from a previous version.
  - Manually through GPO or email, using the MSI file.

In This Chapter

- Installing the Remote Access Clients Hotfix
- Required Gateway Settings
- Configuring a Policy Server
- Remote Access Modes
- Endpoint Security VPN for Unattended Machines (ATMs)
- Automatic Upgrade from the Gateway
- Distributing the Remote Access Clients from a package
- Updating User Sites with the Update Configuration Tool

Installing the Remote Access Clients Hotfix

Install the Endpoint Security VPN R75/Remote Access Clients E75.20 Hotfix on gateways or standalone, self-managed gateway deployments. To use Automatic MEP, install the hotfix on all gateways and the Security Management Server. In a Multi-Domain Security Management environment install the hotfix on the Multi-Domain Server.

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

For other supported gateway versions, install the Hotfix. Find the Hotfix for your gateway version and operating system in sk61286 (http://supportcontent.checkpoint.com/solutions?id=sk61286).

The Remote Access Clients Hotfix enables NGX R65.70 and R70.40 gateways to support E75.20 Remote Access Clients.

To use Implicit MEP, install this hotfix also on the NGX R65.70 and R70.40 Security Management Server.

Note - In environments that require Implicit MEP functionality, the Security Gateways must be the same Check Point version as the Security Management Server, and they must all have the Remote Access Clients Hotfix installed.

To use Implicit MEP in a Multi-Domain Security Management environment, install this hotfix also on the NGX R65.70 and R70.40 Multi-Domain Server.
Before you install the Hotfix:
This Hotfix has possible conflicts with other installed Hotfixes. If you can, it is safest to uninstall all Hotfixes installed on the Security Management Server or gateways. See Uninstalling a Hotfix. If you cannot uninstall a Hotfix, contact Check Point Technical Support.

To install the Hotfix on a Security Gateway or Security Management Server:
3. Run the Hotfix:
   - On SecurePlatform, Disk-based IPSO, and Solaris:
   a) `tar -zxvf <name_of_file>.tgz`
   b) `./UnixInstallScript`
   - On Windows platforms: double-click the installation file and follow the instructions.

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

Required Gateway Settings

You must configure gateways for Remote Access Clients. These procedures are necessary for Remote Access Clients operations.

Note - The screens in these procedures are from SmartDashboard version R71.30. If you are using a different version, there are some differences.

To configure Remote Access Clients management on the gateway:
1. In SmartDashboard, right click the gateway and select Edit.
   The Check Point Gateway window opens.
2. Configure remote VPN functionality:
   - R70 / R71: In the General Properties page, enable the IPSec VPN blade.
3. Add the gateway to the Remote Access VPN community:
   - R71: Open IPSec VPN and click Add.
   - NGX R65 / R70: Open VPN and click Add.
     In the window that opens, click Remote Access and click OK.

4. Set the VPN domain for the Remote Access community.
   a) Open Topology and click Set domain for Remote Access Community.

   b) In the window that opens, select the Remote Access VPN and click Set.

   c) In the window that opens, select a VPN Domain and click OK, or click New and define a VPN domain.
5. Configure **Visitor Mode**.
   - R71: Open **IPSec VPN > Remote Access**.
   - NGX R65 / R70: Open **Remote Access**.
   Select **Visitor Mode** and leave **All Interfaces** selected. You can choose the Visitor Mode **Service**, which defines the protocol and port of Endpoint Security VPN connections to the gateway.

6. Open **Office Mode** and select **Office Mode**.
   - **Office Mode**
     - \( \bigcirc \) Do not offer Office Mode
     - \( \bigcirc \) Offer Office Mode to group: [L2TP-vpn-user] New...
     - \( \bigcirc \) Allow Office Mode to all users
     - **Office Mode Method**
       - Allocate IP address by sequentially trying the checked methods, until success:
         - \( \bigcirc \) From ipaddress.conf located in $FWDIR/conf - always try first
         - \( \square \) From the RADIUS server used to authenticate the user
         - \( \bigcirc \) Using one of the following methods:
           - \( \bigcirc \) Manual (using IP pool)
             - Allocate IP addresses from network: [Remote-1.dzn] New...
           - \( \bigcirc \) Automatic (using DHCP)
             - Use specific DHCP server:
             - Virtual IP address for DHCP server replies:
             - MAC address for DHCP allocator: [Unique per machine]
     - [Optional Parameters...]

   a) Select for a group or for all users.
   b) Select an Office Mode method.
   c) 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:
1. Open the Remote Access Community Properties window:
   - R70 / R71: Open the **IPSec VPN** tab on SmartDashboard.
   - NGX R65: Open the **VPN** tab on SmartDashboard.
2. Double-click the **Remote Access VPN** community.
3. Open **Participant User Groups**. Make sure all Remote Access Clients client users are added.
   - 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.

4. Open Participating Gateways. Make sure the gateway you want to manage Endpoint Security VPN clients is listed.
5. Close OK.

To configure encryption for the VPN:
1. Open Policy menu > Global Properties.
2. Open Encryption Properties.
   - NGX R65 / R70: Open Remote Access > VPN - IKE (Phase 1).
3. In the Support encryption algorithms list, make sure that at least one AES encryption algorithm is selected.
4. In the Use encryption algorithm list, select an enabled AES encryption algorithm.
   
   **Important** - The client does not support DES algorithms. You *must* select an AES algorithm.

   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, right-click the gateway that will serve as the Policy Server and select Edit. The Check Point Gateway window opens.
2. Enable Policy Server functionality:
   - NGX R65: In Check Point Products, click VPN and SecureClient Policy Server.
3. Open Authentication.
4. From the Users drop-down, select an existing user group of remote access clients. Users that authenticate to the gateway must belong to this group.
5. Click OK.
Remote Access Modes

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

Note - Hub mode is not supported in SecuRemote.

To enable Hub Mode:

1. In SmartDashboard, open Policy > 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.

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 103) 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.

Automatic Upgrade from the Gateway

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.

If you have a gateway version that requires the Remote Access Clients Hotfix, make sure that the Hotfix is installed before you put an upgraded package on the gateway.
If you have R71.x with SSL VPN enabled, put the TRAC.cab file in a different directory, as shown in the instructions.

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.

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.
   - For R71.x, back up the TRAC.cab file in:
     $CVPNDIR/htdocs/SNX/CSHELL
3. Put the new TRAC.cab and ver.ini files in the same directory on the gateway:
   - For R71.x, put the TRAC.cab file also in:
     $CVPNDIR/htdocs/SNX/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 the SmartDashboard.
   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.
   - If users had Endpoint Security VPN R75, it keeps the existing settings.
   - If users had Endpoint Connect R73, it automatically upgrades to Endpoint Security VPN.

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:

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.
Distributing the Remote Access Clients from a package

You can create packages of the Remote Access Clients with pre-defined settings, such as which client to install, a VPN site and authentication methods. When you deploy the package to users, it is easier for them to connect quickly.

Remote Access Clients Administration mode lets you create pre-configured packages. You open one instance of the client, configure all settings, and save the client MSI.

Decide if you want to pre-configure the client package, and with which features. Then deploy the MSI package.

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.

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.

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.

If any of the required features are disabled on the client in Administration mode, change the configuration of the gateways ("Global Properties for Remote Access Clients Gateways" on page 52).

Creating the Client Installation Package

It is easiest for users if you pre-configure the MSI package before you distribute it. Create a pre-configured package in Remote Access Clients Administration mode. You open one instance of the client, configure all settings, and save the client MSI. The package can include:

- Which client installs (Endpoint Security VPN, Check Point Mobile for Windows, or SecuRemote
- A VPN site
- The authentication method
- An initial firewall policy

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 create a pre-configured package:

2. Open the MSI file and install a client on your computer.
3. Open the client in Administration mode:
   - 32-bit systems - C:\Program Files\CheckPoint\Endpoint Connect\AdminMode.bat
   - 64-bit systems - C:\Program Files(x86)\CheckPoint\Endpoint Connect\AdminMode.bat
4. Right-click the client icon and select VPN Options.
   The Administration tab of the Options window opens.
5. Select the Sites tab.
6. Define the site that clients will connect to.
7. Select the site and click Properties > Settings.
Distributing the Remote Access Clients from a package

The **Properties** window opens.

8. Configure the VPN options:
   - **Always-Connect** - Let the client connect automatically to the active site.
   - **VPN tunneling** - Make sure the client connects to the VPN for all outbound traffic. Enable Hub Mode for the gateway ("Remote Access Modes" on page 19).
   - **Authentication** ("Authentication Schemes and Certificates" on page 23)

9. Click **OK**.

10. Select the **Advanced** tab and configure settings ("Advanced Client Settings" on page 29) as required for your environment.

11. Select the **Administration** tab.

   ![Endpoint Security Administration Tab](image)

   a) **Input MSI Package Path** - Click **Browse** and select the input MSI package file.

   b) **Replace user’s configuration when upgrading** -
- When cleared, users keep their configuration after the upgrade.
- When selected, the new configuration is merged with the old configuration. Users do not have to apply for new credentials to a site that they have been using.

c) **Enforce default firewall policy after client installation** -
- When cleared, clients that install Endpoint Security VPN only enforce a firewall policy after they connect to the VPN for the first time.
- When selected, when Endpoint Security VPN is installed it will immediately enforce the initial firewall policy. The initial firewall policy is the last policy installed on the computer where the MSI is generated at the time that it is generated. It is enforced until the client connects to the VPN and gets a different policy.

d) For new installations, select a product that users install: Endpoint Security VPN, Check Point Mobile for Windows, or SecuRemote.
- If you do not select a product, users can choose.
- If users already have an E75.x Remote Access Client installed, this will not change the product type.

e) Click **Generate** to create the MSI package.
- A window opens to select a location to save the generated package.
12. Distribute this package to Remote Access Clients users.
13. Users will double-click the MSI file and follow the on-screen instructions.

**Note** - On Windows Vista and Windows 7, there may be a prompt to allow access, depending on the UAC settings.

### Authentication Schemes and Certificates

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

Remote Access Clients support these authentication types:

- Username and password
- Certificate - CAPI (for CAPI certificates and Smart Cards)
- Certificate - P12
- SecurID - KeyFob
- SecurID - PinPad
- SecurID – Software Token
- Challenge Response
- SAA - Username and Password
- SAA - Challenge Response

### Pre-Configuring Authentication Method

From the client, users can change how they authenticate to a VPN gateway. You can preconfigure the client with an authentication method. Make sure to give all users the necessary authentication data or files.

**To change the authentication scheme from the client:**

1. Right-click the client icon and select **VPN Options**.
   - The **Options** window opens.
2. On the **Sites** tab, select a site and click **Properties**.
   - The **Properties** window for the site opens.
   - On the **Settings** tab, select an option from **Authentication Method**.

If you do not want to pre-package the MSI, you can pre-configure the default authentication method in the gateway configuration file.
To configure default authentication for users of a site:

1. On the gateway, open the $FWDIR/conf/trac_client_1.ttm file with a text editor.
2. In the `default_authentication_method` section, change `:default` to one of the following valid values:
   - `client_decide` (let user decide, default)
   - `username-password`
   - `certificate` (for Certificate "CAPI"
   - `p12-certificate`
   - `securIDKeyFob`
   - `securIDPinPad`
   - `SoftID`
   - `challenge-response`
   - `SAA-username-password`
   - `SAA-challenge-response`

3. Save the file and install the policy.

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

   This example shows a configuration for Certificate - P12 authentication.

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

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

Certificates

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

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

Stored in CAPI or Stored as Files

Remote Access Clients support user authentication through PKCS#12 certificates. A PKCS#12 certificate can be accessed directly when stored as a .p12 file or imported to the CAPI store.
CAPI lets Windows-based applications do cryptographic operations. The CAPI store is a repository of digital certificates associated with a Cryptographic Service Provider (CSP). Each CSP controls the cryptographic keys belonging to the certificates.

Decide whether to let users import certificates to the CAPI store:
- Certificates in the CAPI store are easier to manage.
- If a user has several computers, will use a temporary computer, or is using a laptop (that might be stolen), it is better if the certificate is not stored on the computer. Give the user a PKCS#12 certificate on removable media.

Generating and Deploying Certificates
Generate certificates in SmartDashboard:
- Enroll Certificate (Generate Registration Key). Initiate a certificate that will be pending for the user. The result is a registration key. The user completes the creation of the certificate with the registration key. The result can be a certificate stored as a PKCS#12 file or stored in the CAPI.
- Generate PKCS#12 File. Generate a PKCS#12 certificate and save it to a file. The user authenticates with the PKCS#12 file.

Generating Registration Keys
Generate a registration key from SmartDashboard to let users import certificates to the CAPI store.

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

Generating PKCS#12 Files
Generate a certificate file from SmartDashboard.

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

Certificate Enrollment and Renewal

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

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

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

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

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

**To import a certificate through the client:**
1. Right-click the client icon, and select **VPN Options**.
2. On the **Sites** tab, select the gateway and click **Properties**.
3. Open the **Settings** tab.
4. Make sure that **Certificate - CAPI** is selected in the **Method** menu.
5. Click **Import**.
7. Enter the certificate password and click **Import**.

**To import a certificate through Windows file explorer:**
1. Double-click the P12 file.
   The certificate import wizard opens.
2. Click **Next**.
   The path of the file to import is shown.
3. Click **Next**.
4. Enter the password for the private key.
5. Select an option:
   - **Enable strong private key protection** - Users are prompted to enter the password when the private key is used.
   - **Mark this key exportable** - Users can back up and move the key.
6. Click **Next**.
7. Select to import to CAPI store, or browse to a storage folder.
8. Click **Finish**.
Disabling CAPI Authentication

Remote Access Clients support user authentication with PKCS#12 certificates. A PKCS#12 certificate can be accessed directly or imported to the CAPI store.

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

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

   ```
   enable_capi (
     :gateway (  
      :false (false)  
      :true (true)  
      :client_decide (client_decide)  
    )  
     :default (false)  
   )
   ```

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

SecurID

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

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

The Remote Access Clients site wizard supports both methods, as well as softID. Remote Access Clients uses both the PIN and tokencode, or just the passcode, to authenticate to the gateway.

SoftID

SoftID operates the same way as a passcode device, but consists only of software that sits on the desktop.

The Advanced view displays the tokencode and passcode with COPY buttons. This enables the user to cut and paste between softID and the client.

Key Fobs

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

Working with RSA Hard and Soft Tokens

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

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

To configure RSA SoftID:

1. Make a remote user group on the Ace Server.
2. Supply the SDTID token file (or multiple tokens) to the remote users.
3. Instruct remote users on how to import the tokens.
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.

You select Secure Authentication API (SAA) as the authentication method when you create a site or when you create an MSI package. You then select a DLL file to use. The DLL is a file that you create that uses the OPSEC API and other SAA API to interface with the client. When users connect to a site, a window opens based on the SAA authentication type that is configured for the site, and users authenticate seamlessly.

One DLL file is used globally for all sites that use SAA authentication.

Note - Only users with administrator permissions can replace the DLL.

For details of how to create the required DLL file, see Creating a DLL file to use with SAA (on page 110).

Configuring SAA

You can configure SAA in these ways:

- Administrators can select it as the authentication method for a site when they create an installation package with the MSI.
- Users can select it as the authentication method when they create a site.
- An administrator can configure a DLL file for SAA in an installation package. Users can then select SAA authentication for a site and use the DLL that is already configured.

We recommend that administrators configure it for a site or in an installation package to prevent confusion. Users can replace the current DLL file with a new one if changes are necessary.

To configure SAA for an installation package:
1. When you create an installation package, right-click the client icon and select Options.
2. In the Advanced tab, select Use a Secure Authentication API File and browse to select a DLL file.

SAA will not be active until a site is configured to use SAA Authentication. When you or a user configures SAA as the authentication method for a site, the DLL that you inserted is used.

To configure SAA as the authentication method for a site:
1. From the Site Wizard, on the Authentication Method page, select Secure Authentication API (SAA).
   A Secure Authentication API (SAA) page opens.
   
   Secure Authentication API (SAA)
   Select the type of third-party authentication that you use.

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

   ✔ Challenge Response
   Click if you are required to provide different responses to a challenge.

   Use a Secure Authentication API File:
   ![Select a SAA DLL file] Browse...
   Select the Secure Authentication API DLL file supplied by your administrator. If you do not have this, contact your administrator.

2. On the Secure Authentication API (SAA) page, select the type of SAA authentication:
   - Username and Password - Users enter a username and password.
   - Challenge Response - Users enter a response to a challenge.
3. Click **Browse** and select the DLL file. If users will do this step, make sure that they have the correct DLL file.

   **Note** - Only users with administrator permissions can replace the DLL.

4. Click **Next** and **Finish** to complete the site creation.

**SAA From the User’s Perspective**

Usually, when users connect to the site, a login window opens and they enter their authentication information directly in that window. If SAA is the authentication method for the site, there are no fields for authentication information in the login window. Users must click the **Connect** button in the window and a new window opens for authentication information.

After a user authenticates to the site with SAA authentication, the experience is the same as a user who authenticates with a different authentication method.

**Challenge-Response**

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

**Authentication Timeout**

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

**To change Authentication Timeout:**

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

**Advanced Client Settings**

Configure client behavior in the **VPN Options** > **Advanced** tab.

1. Right-click the client icon and select **VPN Options**.
   
   The **Options** window opens.
2. Open the **Advanced** tab.

![Advanced Tab](image)

**Pre-Configuring Logging Options**

Remote Access Clients let users send log files with their default email client. 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.

   ```ttm
   :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.

**Pre-Configuring Proxy Settings**

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

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

If you know that this will be an issue, you can configure this option when you prepare the client MSI file. Otherwise, you can help your user configure the proxy server when the issue comes up.

**To configure proxy settings on the client:**

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

2. Select an option.
   - *No Proxy* - Make a direct connection to the VPN.
   - *Detect proxy from Internet Explorer settings* - Take the proxy settings from Internet Explorer > Tools > Internet options > Connections > LAN Settings.
   - *Manually define proxy* - Enter the IP address and port number of the proxy. If necessary, enter a valid user name and password for the proxy.
3. Click **OK**.

Pre-Configuring Client Interface Language

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

*To change the interface language:*
1. Open the **Options** > **Advanced** tab.
2. From the **Choose the interface language** drop-down menu, select the language you want.

Pre-Configuring SDL Enable

You can enable SDL (**Secure Domain Logon (SDL)** on page 45) for the Remote Access Clients.

*To enable SDL in the client:*
1. Open the **Options** > **Advanced** tab.
2. Click **Enable Secure Domain Logon**.

Replacing the DLL File

One DLL file is used globally for all sites that use SAA authentication. This file is stored in each local client installation. Users can replace the DLL on their local installations if changes are necessary.

*Note* - Only users with administrator permissions can replace the DLL.

*To replace the local DLL file:*
1. Right-click the client icon and select **Options**.
2. In the Advanced tab, next to Use a Secure Authentication API File, browse to select the new DLL file. This file is used for SAA authentication.

**Editing an MSI Package with CLI**

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**

```plaintext
cpmsi_tool <MSI-package-file-name>
[<-in|out|-add|-remove|-overwrite|-copyout|-add_scv_plugin|-remove_scv_plugin|-overwrite_scv_plugin> <filename>]
[-replace_config <true|false>] [-sql_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>
</table>
| -in                | Add <filename> to the package. The file can be a filename from the list below, or "all" for all of them. The file must exist in same directory as the MSI file. Possible files:  
  - LangPack1.xml  
  - DisconnectedPolicy.xml  
  - Trac.config |
| -out               | Remove <filename> from the package. The file can be a filename from the list below, or "all" for all of them. The file must exist in same directory as the MSI file. Possible files:  
  - LangPack1.xml  
  - DisconnectedPolicy.xml  
  - Trac.config |
| -add               | Add <filename> to the package. The file can be any file. It must exist in same directory as the MSI file. |
| -remove            | Remove a file <filename>, that you added previously, from the MSI. |
| -overwrite         | Overwrite <filename> with a new version of the file. It must be a file that was added. |
| -copyout           | Save <filename> as a separate file. |
| -add_scv_plugin    | Add a third party SCV plugin file to the package. <filename> is the name of the SCV plugin. The file must exist in same directory as the MSI file. |
| -remove_scv_plugin | Remove a third party SCV plugin file from the package. <filename> is the name of the SCV plugin. |
| -overwrite_scv_plugin | Overwrite a third party SCV plugin file that was added to the package previously. |
| -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 SDL  
  Possible values: true or false  
  true - Secure Domain Logon (SDL) is enabled for the package. |
| -fixed_mac         | Possible values: true or false  
  true - The client will use fixed Office mode MAC addresses. |
| -ClientSubType     | Default client type.  
  Possible values: SecuRemote | CheckPointMobile | EndpointSecurityVpn | UserDecide |
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

<table>
<thead>
<tr>
<th>Type of Installation</th>
<th>Command</th>
<th>Notes on Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regular</strong> - 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.</td>
<td><code>\&quot;C:\WINDOWS\system32\msiexec.exe&quot; /i &quot;C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi&quot; /qb! INSTALLDIR=&quot;C:\Program Files\CheckPoint\Endpoint Connect&quot;</code></td>
<td>qb! - Basic UI level</td>
</tr>
<tr>
<td><strong>Silent</strong> - Use this for an ATM installation. User interface shows on the screen but users do not press anything. If necessary, the client automatically restarts.</td>
<td><code>\&quot;C:\WINDOWS\system32\msiexec.exe&quot; /i &quot;C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi&quot; /qb! INSTALLDIR=&quot;C:\Program Files\CheckPoint\Endpoint Connect&quot;</code></td>
<td>qb! - No user interaction is required</td>
</tr>
<tr>
<td><strong>No User Interface</strong> - All user interface is hidden.</td>
<td><code>\&quot;C:\WINDOWS\system32\msiexec.exe&quot; /i &quot;C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi&quot; /qn INSTALLDIR=&quot;C:\Program Files\CheckPoint\Endpoint Connect&quot;</code></td>
<td>qn - no UI</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 35).

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</td>
<td>The path on the user’s machine to the temporary location where they put the</td>
</tr>
<tr>
<td>and path</td>
<td>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.
Updating User Sites with the Update Configuration Tool

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
   ```
Chapter 3

Helping Your Users

This chapter is a summary of basic actions that end-users do when they install and use Remote Access Clients. For more details see the User Guide for that client.

In This Chapter

| Simple Installation | 37 |
| Remote Access Clients Client Icon | 37 |
| Helping Users Create a Site | 38 |
| Helping Users with Basic Client Operations | 40 |

Simple Installation

Users can easily install Remote Access Clients 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).

Remote Access Clients Client Icon

The Remote Access Clients client icon shows the status of the client.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Disconnected]</td>
<td>Disconnected</td>
</tr>
<tr>
<td>![Connecting]</td>
<td>Connecting</td>
</tr>
<tr>
<td>![Connected]</td>
<td>Connected</td>
</tr>
<tr>
<td>![Encryption]</td>
<td>Encryption (encrypted data is being sent or received on the VPN)</td>
</tr>
<tr>
<td>![Issue]</td>
<td>There is an issue that requires users to take action.</td>
</tr>
</tbody>
</table>
Helping 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 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-1 Fingerprint.
5. Send the fingerprint to users before they install the client.

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.

The wizard shows the progress while the Client resolves the site name or address to the actual gateway. This step in the wizard notifies the user that:

This may take several minutes, depending on the speed of your network connection.

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

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

b) Click Details to see additional warnings.

c) If site details are correct, click Trust and Continue. The fingerprint is stored in the Windows registry and the security warning is not opened again for the site, even if the client is upgraded.

The wizard displays the authentication method step.

3. Give your users the authentication materials they need ("Authentication Schemes and Certificates" on page 23).

4. The user selects the correct method and clicks Next.

   • 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.

5. The user clicks Finish and a message shows: Would you like to connect?

   If the user clicks Yes, the client connects to the gateway and a VPN tunnel is created.

Opening the Site Wizard Again

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

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

1. 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
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 right-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.</td>
</tr>
</tbody>
</table>
| Shutdown Client | Closes the Client.  
An open VPN is closed. A background service continues to run and responds to CLI commands. To stop the service: `net stop tracsrvwrapper`  
If you close Endpoint Security VPN and stop the service, the desktop firewall still enforces the security policy. |
Chapter 4

Configuring Client Features

After you configure a feature, make sure to install the policy to apply the changes to clients.

In This Chapter

- Installing Desktop Security Policy
- Managing Desktop Firewalls
- Secure Domain Logon (SDL)
- Multiple Entry Point (MEP)
- Secondary Connect
- Global Properties for Remote Access Clients Gateways
- Split DNS
- Configuring Log Uploads
- Configuring Post Connect Scripts
- Office Mode IP Address Lease Duration
- Supported Algorithms

Installing Desktop Security Policy

To install the Desktop Security policy (for Endpoint Security VPN only):
1. Click Policy menu > Install.
2. In the Install Policy window, select Desktop Security for the Endpoint Security VPN gateway.
   - If this column is not available, you did not configure the Policy Server. This is necessary.
3. Click OK.
   - When clients download the new policy from the gateway, configuration changes are applied.

Managing Desktop Firewalls

Note - The Check Point Desktop Firewall works with the Endpoint Security VPN client. It does not work with SecuRemote or Check Point Mobile for Windows.
In This Section

The Desktop Firewall
Rules
Default Policy
Logs and Alerts
Wireless Hotspot/Hotel Registration
Planning Desktop Security Policy
Operations on the Rule Base
Making the Desktop Security Policy
Letting Users Disable the Firewall

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.

<table>
<thead>
<tr>
<th>Endpoint Security VPN Desktop Policy Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security Management Server</td>
</tr>
<tr>
<td>2. Gateway</td>
</tr>
<tr>
<td>3. Endpoint Security VPN client</td>
</tr>
</tbody>
</table>

Rules

The Desktop Security Policy has Inbound and Outbound rules.

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

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

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

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

- The implicit **outbound** rule allows all connections originating from the client to go out, if they do not match previous blocking rules:
  
  \[ \text{Any Destination, Any Service} = \text{Accept}. \]

- The implicit **inbound** rule blocks all connections coming to the client that do not match previous rules:
  
  \[ \text{Any Source, Any Service} = \text{Block}. \]

**User Granularity**

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

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

- **User Groups** - Set rules to be implemented for some users and not others. For example, define restrictive rules for most users, but give system administrators more access privileges.

Rules are applied to user groups, not individual users. Endpoint Security VPN does not inherently identify user groups, so it must obtain group definitions from the gateway. The gateway resolves the user groups of the authenticated user and sends this information to the Endpoint Security VPN client. Endpoint Security VPN enforces the rules applicable to the user, according to groups. Rules can also be applied to radius groups on the RADIUS server.

**Default Policy**

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

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

**Logs and Alerts**

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

- 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 ("Pre-Configuring Proxy Settings" on page 30) might be required.
Planning Desktop Security Policy

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

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

Operations on the Rule Base

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

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

Making the Desktop Security Policy

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

**To make a Desktop Security Policy:**
1. Open the Desktop tab.
2. Configure the rules. For each rule, you can specify users for whom the rule is applied.
   - 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.

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 E75.20 Upgrade Guides.

Making a Rule for FTP

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

**To add the Active FTP Rule:**
1. In SmartDashboard, open the Desktop tab.
2. Right-click the Outbound rules and select Add.
3. In the rule, select one of the FTP services as the service and Allow as the action.
Letting Users Disable the Firewall

You can configure if Endpoint Security VPN users can choose to disable the firewall policy on their local machines. By default Endpoint Security VPN users do have this option.

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` (default) - 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 45
- Configuring Windows Cached Credentials 46
- Using SDL in Windows XP 46
- SDL in Windows Vista and Windows 7 46

Configuring SDL

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

To create an SDL-enabled client:
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.

Using SDL in Windows XP

To use SDL in Windows XP:
1. When the Windows Logon window is open, the user enters the operating system credentials and clicks OK.
   The Remote Access Clients Logon window opens.
2. The user enters the Remote Access Clients credentials.
   If logon fails and no cached information is used, wait one minute and try again.
   You can customize the Remote Access Clients installation packages with SDL enabled by default.

SDL in Windows Vista and Windows 7

There are different SDL modes for Windows Vista and Windows 7.

- 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.

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.

Note - Implicit mode SDL is not invoked with smart card logon to Windows.
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.
  
  Remote Access 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** - Remote Access Clients randomly select a gateway.

  Recommendation: If you have multiple gateways of equal performance. The traffic of Remote Access Clients is shared between the gateway. 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 give 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:

```plaintext
: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:
- NGX R65 and R70: VPN Basic
- R71 and higher: 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 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 network objects tree, **Groups** section, create a group of gateways to act as backup gateways.

3. Open the VPN properties of the Primary gateway:
   - NGX R65 and R70: **Gateway properties** > **VPN**
   - R71 and higher: **Gateway properties** > **IPSec VPN**
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) On the **Properties** window of the backup network object > **Topology** > **VPN Domain** section, select **Manually defined**.
     c) Select the group.
6. Click **OK**.
7. 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.

**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 50).
   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`.
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 49).
   - 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.

Secondary Connect is compatible with legacy SecureClient settings.

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.ttf 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:

   ```
   :enable_secondary_connect(
     :gateway (  
       :map (  
         :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.

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 SmartDashboard.
2. Open Policy > Global Properties.
4. Set Authentication Settings (on page 53).
5. Set Connectivity Settings.
Global Properties for Remote Access Clients Gateways

- Connect Mode (on page 53)
- Location Aware Connectivity (on page 54)
- Disconnect when connectivity to network is lost ("Roaming" on page 53)
- Disconnect when device is idle ("Idle VPN Tunnel" on page 56)

7. Set Client upgrade mode ("Configuring Upgrades" on page 20).
8. Click OK.
9. Install the policy.

**Authentication Settings**

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

**To configure authentication settings:**

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

- Cache password for - Password retention period in minutes (default = 1440), if password caching is enabled.
  
  **Note** - For security reasons, the cache is cleared when the user explicitly disconnects, even if the cache period has not ended.

  The cache is useful for re-authentications and automatic connections triggered by the Always-Connect feature.

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

**Connect Mode**

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

- Manual - VPN connections are not initiated automatically. Users select a site and authenticate every time they need to connect.
- Always connected - 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_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 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.
  The Interface-topology-based setting was introduced in Check Point NGX R65 HFA 60 and is the preferred method. It is reliable and requires no special configuration, but it has no GUI (it uses GuiDBedit). If you have Check Point NGX R65 HFA 60, this setting requires the NGX R66 plug-in for Connectra on the management server.

- **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

Before you begin: If you have NGX R65, make sure that the NGX R66 plug-in for Connectra is installed on the SmartCenter server.

**To enable location awareness:**
1. In SmartDashboard, 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.
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, 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."

### Configuring Location Awareness for NGX R65 Gateways

On R65 SmartCenter servers without the Connectra R66 plug-in, Location Awareness does not appear in the SmartDashboard. You must configure the settings manually through trac_client_1.ttm. After you install the plug-in, most of the Location Awareness settings appear in the SmartDashboard or GuiDBedit. The values in the TTM file for these settings are ignored, and the file is not updated with values set in the SmartDashboard.

**To configure location awareness in the configuration file:**

1. Open `$FWDIR/conf/trac_client_1.ttm` on the gateway.
2. Enable location awareness:
   - `location_awareness_enabled - set to client_decide or true`
3. Set the parameters under the `:default` attribute of each parameter described:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>la_detect_wlan_as_external</td>
<td>Set to True to make sure wireless networks are treated as external locations, except for the internal wireless networks that you define as internal</td>
</tr>
<tr>
<td>la_wlan_networks_exceptions</td>
<td>Enter the list of internal wireless networks.</td>
</tr>
<tr>
<td>la_defined_dns_suffixes</td>
<td>Enter the list of internal DNS suffixes to make sure unknown DNS suffixes are treated as external locations. (This parameter is applied only if the list is not empty.)</td>
</tr>
<tr>
<td>la_prefer_dc_over_internal_network</td>
<td>Set to True to find the location according to the Domain Controller, or leave as False to use the internal network configuration.</td>
</tr>
<tr>
<td>la_cache_external_networks</td>
<td>Set to True to let the client save the detected external networks in a cache, for faster location awareness.</td>
</tr>
</tbody>
</table>

If you configure a list, for example in `la_wlan_networks_exceptions` and `la_defined_dns_suffixes`, use the delimiter `&` between the items in the list. For example, `checkpoint.com&zonelabs.com&example.com`.

1. Save the file.
2. Install the policy.

### 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). Remote Access 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 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.

   ```
   :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.

To enable hotspot registration from SmartDashboard:

2. Select **Enable registration**.
3. Set the **Maximum** time and add **Ports** to be used.
4. Select a **Track** option.
   The **Local subnets access** and **Allow access** options are not supported in Remote Access Clients.
5. Click **OK**.
6. Save and install the policy.

   \[\text{Note - Local subnet access only and Allow access to maximum of: are not supported for this release.}\]

### 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. Open the `$FWDIR\conf\trac_client_1.ttm` file on the gateway.

   ```plaintext
   :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 and install the policy.

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

### 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. In SmartDashboard, go to the **Servers and OPSEC Applications** tab of the Objects Tree.
2. Right-click **Servers** and select **New SecuRemote DNS**.
The **SecuRemote DNS Properties** window opens.

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

4. In the **Domains** tab, click **Add** to add the domains that will be resolved by the server.

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

6. 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".

7. Click OK two times to complete the configuration.

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:

   ```
   :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 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 hidden window (default: `false`).
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 renegotiation, 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.

Supported Algorithms and

These algorithms are supported by Remote Access Clients to use with IKE:
- 3DES
- AES-128
- AES-256
- MD5
- Sha-1
- Diffie-Helman Group2 (1024)

These transport protocols are supported by Remote Access Clients:
- NAT traversal with UDP encapsulation, with allocated port set to `UDPVPN1_IPSEC_encapsulation`.
- Visitor Mode through TCP connection with predefined port. By default, port 443.
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.

In This Chapter

Check Point SCV Checks 61
Configuring the SCV Policy 62
Configuring SCV Enforcement 62
Configuring SCV Exceptions 63
Traditional Mode 63
Installing and Running SCV Plugins on the Client 63
SCV Policy Syntax 64
Deploying a Third Party SCV Check 86

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.
- **HWMonitor** - Verifies CPU type, family, and model.
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, 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. In SmartDashboard, select Policy > Global Properties.
3. Select **Apply Secure Configurations on Simplified Mode**.
   This causes the gateway to verify client compliance.

   Simplified Mode supports VPN communities. If you must use Traditional Mode, configure SCV enforcement in the Rule Base.

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.
Configuring SCV Exceptions

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 SmartDashboard:
   - 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:

```scv
t :browser_major_version (7)
t :browser_minor_version (0)
t :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.

```scv
begin_or
begin_or (or#) - end (or#)
begin_or (or#)
 :browser_major_version (5)
 :browser_major_version (6)
end(or#)
```

This section checks if the version of Internet Explorer is 6 OR 7. If it is one or the other, the section is true.

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

```
: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)
:begin_or (or1)
```

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

```
send_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.

This option was supported in SecureClient. It is not supported in Remote Access Clients.

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 brace.

**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”, “VirusScan”, “McAfee”, “OfficeScan”, or “ZoneLabs”.</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”)</td>
</tr>
<tr>
<td></td>
<td>- TrendMicro Officescan example: “&lt;650”</td>
</tr>
<tr>
<td></td>
<td>- McAfee VirusScan example: (“&gt;404291”) 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><code>browser_major_version (#)</code></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><code>browser_minor_version (#)</code></td>
<td>Internet Explorer minor version number.</td>
</tr>
<tr>
<td><code>browser_version_operand (&quot;\&gt;\&quot;)</code></td>
<td>The operator used for checking the Internet Explorer's version number.</td>
</tr>
<tr>
<td><code>browser_version_mismatchmessage</code></td>
<td>Message to be displayed for a non-verified configuration of Internet Explorer.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>restricted_download_files (disable)</td>
<td>The maximum permission level that IE should have for downloading files from restricted zones.</td>
</tr>
<tr>
<td>restricted_java_permissions (disable)</td>
<td>The maximum security level that IE should have for running java applets from restricted zones.</td>
</tr>
</tbody>
</table>
| send_log (type)                                     | Whether to send a log to Security Management server for specifying that the client is not verified: log or alert.  
Does not support begin_admin.                        |
| internet_options_mismatch_message (“Your Internet Browser settings do not meet policy requirements”) | Mismatch message for the Internet Explorer settings.                                                                                  |

**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: “823980(true)” 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: “KB823980(true)” 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: “GenuineIntel&quot;, or “AuthenticAMD&quot;, or “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>cpumodel(9)</td>
<td>The CPU model.</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 (&quot;Your screen saver settings do not meet policy requirements&quot;)</td>
<td>Mismatch message for the screen saver check. The screen saver will not be checked if the property &quot;enforce_screen_saver_minutes_to_activate&quot; 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 (&quot;\geq&quot;)</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 (&quot;\geq&quot;)</td>
<td>Operator for checking the operating system’s service pack on Windows XP.</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;\eq&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;\geq&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;\eq&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>
### SCV Policy Syntax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_pack_version_operand_vista (&quot;=&gt;&quot;)</td>
<td>Operator for checking the operating system’s service pack on Windows Vista.</td>
</tr>
<tr>
<td>os_version_mismatches (&quot;Please upgrade your operating system&quot;)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**ProcessMonitor**

This check is for process activity. It supports AND and OR sections.

The only parameter is the name of the process to check.

- **ProcessName.exe** *(true | false)*
  - 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.

**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")
      :begin_and (and1)
        :string ("Software\Microsoft\Internet Explorer\Version>=7")
    :begin_and (and1)
      :string ("Software\Microsoft\Internet Explorer\Version>=6.0")
)
```
:string ("Software\Microsoft\Windows\CurrentVersion\Internet Settings\MinorVersion>=SP2") :end_and (and1) :begin_and (and2) :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 &quot;vvshhhbbb&quot;. 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>exe (&quot;c:\Users\nonadmin\script.exe&quot;)</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>script_run_cycle (#)</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 second by default and by default the script runs after every cycle (1).</td>
</tr>
<tr>
<td>run_as_admin (no)</td>
<td>Determines if the script runs with Administrator or User permissions. The default is &quot;no&quot;. If the value is &quot;yes&quot; the script runs with Administrator permissions.</td>
</tr>
<tr>
<td>run_timeout (#)</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>NetworkFirewallRequired</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>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>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>- <strong>any</strong> - Checks if there is any Anti-spyware installed on the endpoint machine (registered in the Windows Security Center).</td>
</tr>
<tr>
<td></td>
<td>- <strong>list of Anti-spyware products separated by a &quot;;&quot; delimiter</strong> - Checks if one of the Anti-spyware products on the list is installed on the endpoint machine.</td>
</tr>
<tr>
<td></td>
<td>- <strong>none</strong> - Disables the check</td>
</tr>
<tr>
<td></td>
<td>This check is not supported on Windows XP. If you configure it, it will run on Windows 7 and Vista but not on XP.</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>- <strong>true</strong> - Enables the check.</td>
</tr>
<tr>
<td></td>
<td>- <strong>false</strong> - Disables the check.</td>
</tr>
<tr>
<td>&lt;CheckName&gt;MismatchMessages</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>
<tr>
<td>PassCheckWhenSecurityCenterIsUnavailable</td>
<td>Can override the WindowsSecurityMonitor checks if the Windows Security Center is not working. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- <strong>true</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>false</strong> - (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.</td>
</tr>
<tr>
<td>MinutesForWscsvToStart(x)</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### 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

```
SCVEpsNames (
    : (WindowsSecurityMonitor
        :type (plugin)
        :parameters (
            :VirusProtectionRequired (true)
            :VirusProtectionRequiredMismatchMessage ("Please see that your AntiVirus is updated and active")
            :VirusProtectionInstalledPrograms ("Trend Micro OfficeScan Antivirus;Kaspersky Anti-Virus")
            :VirusProtectionInstalledProgramsMismatchMessage ("Please see that your AntiVirus is Trend Micro or Kaspersky")
            :WindowsUpdateRequired (true)
            :WindowsUpdateRequiredMismatchMessage ("Please turn on Windows automatic Updates")
            :SpywareProtectionRequired (true)
            :SpywareProtectionRequiredMismatchMessage ("AntiMalware is not updated or active")
            :SpywareProtectionInstalledPrograms ("none")
            :SpywareProtectionInstalledProgramsMismatchMessage (""")
            :NetworkFirewallRequired (true)
            :NetworkFirewallRequiredMismatchMessage ("Please check the your network firewall is turned on")
            :NetworkFirewallInstalledPrograms ("Kaspersky Anti-Virus")
            :NetworkFirewallInstalledProgramsMismatchMessage ("Please check that Kaspersky Anti-Virus firewall is installed on your machine"
        )
    )
)
```

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.

1. On the Security Management Server, open \$FWDIR\conf\local.scv.
2. In the SCVGlobalParams section, set the value of disconnect_when_not_verified.
   - **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.

1. On the Security Management Server, open $FWDIR\conf\local.scv.
2. In the **SCVGlobalParams** section, find **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 **not_verified_script_run_show**.
   - **True** - The user will see the script running.
   - **False** - The script run will be hidden. (default)
5. Set the value **not_verified_script_run_admin**.
   - **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 **not_verified_script_run_always**.
   - **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:**

1. On the Security Management Server, open $FWDIR\conf\local.scv.
2. In the **SCVGlobalParams** section, set the value of **scv_checks_interval** with a value that is a number in 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.
   - 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:**

1. On the Security Management Server, open $FWDIR\conf\local.scv.
2. In the **SCVGlobalParams** section, set the value of **skip_firewall_enforcement_check** to **true**.
3. Install the desktop policy in SmartDashboard.
   - 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, the allow non SCV client option is disabled.

To enable Allow non SCV Clients in the global parameters:
1. On the Security Management Server, open $FWDIR\conf\local.scv.
2. In the SCVGlobalParams section, set the value of allow_non_scv_clients to true.
3. Install the desktop policy in SmartDashboard.
   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.

```xml
(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_mismatchmessage ("Please upgrade your Internet browser.")
         :intranet_download_signedactivex (disable)
         :intranet_runactivex (disable)
         :intranet_download_files (disable)
         :intranet_java_permissions (disable)
         :trusted_download_signedactivex (disable)
         :trusted_runactivex (disable)
         :trusted_download_files (disable)
         :trusted_java_permissions (disable)
   )
```
:internet_download_signedactivex (disable)
:internet_runactivex (disable)
:internet_downloadfiles (disable)
:internet_java_permissions (disable)
:restricted_download_signedactivex (disable)
:restricted_runactivex (disable)
:restricted_downloadfiles (disable)
:restricted_java_permissions (disable)
:send_log (alert)

:internet_options_mismatch_message ("Your Internet browser 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.
")

: (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 (">=")
:maj_os_version_number_2003 (5)
:min_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 (">=")

:calc.exe (false)
:begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("Please make sure calc.exe is not running!")
:send_log (alert)
:begin_admin (admin)

: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. Make sure you are logged on as an authorized user.")
  :securely_configured_no_active_user (false)
:securely_configured_no_active_user (false)
:begin_or (or1)
  :begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("Please make sure calc.exe is not running!")
:begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("You are using SecureClient with a non-authorized user. Make sure you are logged on as an authorized user.")
  :securely_configured_no_active_user (false)
:securely_configured_no_active_user (false)
:begin_or (or1)
  :begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("Please make sure calc.exe is not running!")
:begin_admin (admin)
  :send_log (alert)
  :mismatchmessage ("You are using SecureClient with a non-authorized user. Make sure you are logged on as an authorized user.")
  :securely_configured_no_active_user (false)
:securely_configured_no_active_user (false)
: (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)
)
)
: (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.")
)
:end (admin)

)

)

: (RegMonitor

:type (plugin)

:parameters (

:value ("Software\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.\PatternVer>=414")

:begin_admin (admin)

:send_log (alert)

:mismatchmessage ("Please update your AntiVirus (use the LiveUpdate option.")"

):

end (admin)

)

)

: (SCVMonitor

:type (plugin)

:parameters (

:scv_version ("54014")

:begin_admin (admin)

:send_log (alert)

:mismatchmessage ("Please upgrade your Secure Configuration Verification products package.")

):

end (admin)

)

)

: (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)  
      :WindowsUpdateRequiredMismatchMessage ()  
      :SpywareProtectionRequired (true)  
      :SpywareProtectionRequiredMismatchMessage ("Please verify that your spyware protection is turned on.")  
      :SpywareProtectionInstalledPrograms (any)  
      :SpywareProtectionInstalledProgramsMismatchMessage ("There is no anti-spyware program installed on the machine.")  
      :NetworkFirewallRequired (true)  
      :NetworkFirewallRequiredMismatchMessage ("Please verify the your network firewall is turned on.")  
      :NetworkFirewallInstalledPrograms ("Kaspersky Anti-Virus")  
      :NetworkFirewallInstalledProgramsMismatchMessage ("Please verify that the firewall of Kaspersky Anti-Virus is installed on the machine.")  
    )  
  )
)
)
:SCVEpsPolicy (  
  : (WindowsSecurityMonitor)
)
:SCVPolicy (  
  : (ProcessMonitor)
)
:SCVGlobalParams (  
  :enable_status_notifications (false)  
  :status_notifications_timeout (10)  
  :disconnect_when_not_verified (false)  
  :skip_firewall_enforcement_check (false)  
  :block_connections_on_unverified (false)  
  :scv_policy_timeout_hours (168)  
  :enforce_ip_forwarding (false)  
  :not_verified_script ("")  
  :not_verified_script_run_show (false)  
  :not_verified_script_run_admin (false)  
  :not_verified_script_run_always (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 32). When clients install the MSI they automatically get the DLL.

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

See the Remote Access Clients SCV SDK (http://www.opsec.com/cp_products/90.htm) for full details.

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 on the gateway from the SmartDashboard.
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.
Chapter 6

The Configuration File

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

In This Chapter

- Editing the TTM File 87
- Centrally Managing the Configuration File 87
- Understanding the Configuration File 88

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 from SmartDashboard or the CLI of each gateway:
   - In SmartDashboard, select Policy > Install and install Network Security 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:

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, 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

This table shows some of the parameters of the TTM file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Recommended value for :default ()</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow_disable_firewall</td>
<td>Show a menu option for user to enable or disable the desktop firewall.</td>
<td>false</td>
</tr>
<tr>
<td></td>
<td>Applied only if <code>enable_firewall</code> is true or <code>client_decide</code>.</td>
<td></td>
</tr>
<tr>
<td>certificate_key_length</td>
<td>Certificate enrollment settings.</td>
<td>1024</td>
</tr>
<tr>
<td>certificate_strong_protection</td>
<td>Certificate enrollment settings.</td>
<td>true</td>
</tr>
<tr>
<td>certificate_provider</td>
<td>Certificate enrollment settings.</td>
<td>&quot;Microsoft Enhanced Cryptographic Provider v1.0&quot;</td>
</tr>
<tr>
<td>internal_ca_site</td>
<td>Certificate enrollment settings.</td>
<td>none</td>
</tr>
<tr>
<td>internal_ca_dn</td>
<td>Certificate enrollment settings.</td>
<td>none</td>
</tr>
<tr>
<td>default_authentication_method</td>
<td>Default authentication method. If this value exists, users do not select an authentication method when they create sites.</td>
<td>none</td>
</tr>
<tr>
<td>disconnect_on_smartcard_removal</td>
<td>Enable/disable client disconnection when Smart Card with current certificate is removed.</td>
<td>false</td>
</tr>
<tr>
<td>do_proxy_replacement</td>
<td>Enable/disable proxy replacement.</td>
<td>true</td>
</tr>
<tr>
<td>enable_capi</td>
<td>Enable/disable CAPI authentication.</td>
<td>true</td>
</tr>
<tr>
<td>enable_firewall</td>
<td>Enable/disable desktop firewall</td>
<td>true</td>
</tr>
<tr>
<td>enable_gw_resolving</td>
<td>Enable/disable DNS resolution on each connection.</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>Used for MEP.</td>
<td></td>
</tr>
<tr>
<td>flush_dns_cache</td>
<td>Enable/disable flushing the DNS cache while connecting.</td>
<td>false</td>
</tr>
<tr>
<td>hotspot_detection_enabled</td>
<td>Enable/disable automatic hotspot detection.</td>
<td>true</td>
</tr>
<tr>
<td>automatic_mep_topology</td>
<td>Enable/disable the implicit (automatic) MEP method.</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>False - manual MEP method.</td>
<td></td>
</tr>
<tr>
<td>ips_of_gws_in_mep</td>
<td>gateway IP addresses for clients to connect to.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>Applied only if <code>automatic_mep_topology</code> is false.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Addresses are separated by &quot;,#&quot;, and the list is terminated by a final &quot;,#&quot;:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NNN.NNN.NNN.NNN#MMM.MMM.MMM.MMM&amp;M#</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Recommended value for :default ()</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>mep_mode</td>
<td>MEP mode, priority of gateways defined in ips_of_gws_in_mep. Applied only if automatic_mep_topology is false. Valid values: • dns_based • first_to_respond • primary_backup • load_sharing</td>
<td>dns_based</td>
</tr>
<tr>
<td>predefined_sites_only</td>
<td>Enable/disable user ability to create or modify sites.</td>
<td>false</td>
</tr>
<tr>
<td>send_client_logs</td>
<td>Email addresses to which debug logs are sent.</td>
<td>none</td>
</tr>
<tr>
<td>suspend_tunnel_while_locked</td>
<td>Enable/disable traffic suspension if the machine becomes inactive (due to lock or sleep) for a specified duration.</td>
<td>false</td>
</tr>
<tr>
<td>tunnel_idleness_ignore_icmp</td>
<td>Enable/disable monitor of ICMP packets to see if a tunnel is active.</td>
<td>true</td>
</tr>
<tr>
<td>tunnel_idleness_ignored_tcp_ports</td>
<td>TCP ports that are not monitored to determine if a tunnel is active.</td>
<td>none</td>
</tr>
<tr>
<td>tunnel_idleness_ignored_udp_ports</td>
<td>UDP ports that are not monitored to determine if a tunnel is active.</td>
<td>53�����</td>
</tr>
<tr>
<td>tunnel_idleness_timeout</td>
<td>Time, in minutes, after which a client will close an inactive tunnel. Zero (0) - the feature is disabled. The VPN tunnel will never close due to inactivity.</td>
<td>0</td>
</tr>
</tbody>
</table>
Chapter 7

Monitoring and Troubleshooting

In This Chapter

- SmartView Tracker and Remote Access Clients
- Collecting Logs
- Remote Access Clients Files
- "Unsupported Services" Message
- Configuring No-Router Environments
- Connection Terminates
- Troubleshooting the Firewall
- Troubleshooting SCV
- Traffic Dropped for Anti-spoofing
- MEP

SmartView Tracker and Remote Access Clients

To see alerts from Remote Access Clients:
1. Open SmartView Tracker.
3. Double-click an item to open the Record Details window and see more data.

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.

Remote Access Clients let users send log files with their default email client. 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.
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</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>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></td>
</tr>
</tbody>
</table>
"Unsupported Services" Message

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<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>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>

"Unsupported Services" Message

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

**Causes**  
Remote Access Clients do not recognize all services that may be 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.

Configuring No-Router Environments

You must configure the server in SmartDashboard 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 Office Mode:
   - R71: IPSec VPN > Office Mode
   - NGX R65 and R70: Remote Access > 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, open the Gateway Properties window of the Remote Access Clients gateway.
2. Open Office Mode:
   - R71: IPSec VPN > Office Mode
   - R70 and NGX R65: Remote Access > 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

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>
<tr>
<td>Example Output</td>
<td>STATE : 4 Running &lt;STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN&gt;</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.
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</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
Overlapping Encryption Domains

Domains of Gateway A and Gateway B do not overlap, but 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.
Appendix A

Remote Access Clients Command Line

In This Appendix

Using the Command Line 103
CLI Commands 103

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
2. Browse to the Remote Access Clients directory:
   - 32-bit system - C:\Program Files\CheckPoint\TRAC
   - 64-bit system - C:\Program Files(x86)\CheckPoint\TRAC
3. Run: `trac <command> <arg>`.

CLI Commands

These commands can be used for Remote Access Clients.

<table>
<thead>
<tr>
<th>change_p12_pwd</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Arguments</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**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   | pathname 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**

**Description**
Connects to the gateway. If a user's authentication credentials are not cached, it opens the login page so the user can authenticate.

**Syntax**
```
trac connectgui
```

**Arguments**
None

**create**

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

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

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

**Example**

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

### delete

**Description** Deletes a site definition.

**Syntax**

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

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

**Example**

```
trac delete -s mygateway.domain.com
```

### disable_log

**Description** Stops logging.

**Syntax**

```
trac disable_log
```

**Arguments** none

### disconnect

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

**Syntax**

```
trac disconnect [-g <gateway>]
```

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

### enable_log

**Description** Enables logging.
enable_log

Syntax
trac enable_log

Arguments
none

enroll_capi

Description
Enrolls a CAPI certificate.

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>
<tr>
<td>-i</td>
<td>where to store the certificate</td>
</tr>
<tr>
<td></td>
<td>(If you do not enter this in the command, the output shows the options.)</td>
</tr>
<tr>
<td>-l</td>
<td>length of the registration key</td>
</tr>
<tr>
<td>-sp</td>
<td>whether strong key protection is used</td>
</tr>
<tr>
<td></td>
<td>(Valid values: &quot;true&quot; or &quot;false&quot;)</td>
</tr>
</tbody>
</table>

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

help

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

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

**Arguments**
one, but if a command is given, help for that command is shown

### info

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

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

**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></td>
<td>If given, only gateways and tunnel information for this site are shown.</td>
</tr>
</tbody>
</table>

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

### List

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

**Syntax**
```
trac List
```

**Arguments**
one

**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**
one

**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**
```
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>-s</td>
<td>name of the site</td>
</tr>
<tr>
<td>-d</td>
<td>-d</td>
<td>certificate subject name</td>
</tr>
<tr>
<td>-l</td>
<td>-l</td>
<td>length of the registration key</td>
</tr>
<tr>
<td>-sp</td>
<td>-sp</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>-s</td>
<td>name of the site</td>
</tr>
<tr>
<td>-f</td>
<td>-f</td>
<td>pathname for the certificate file</td>
</tr>
<tr>
<td>-p</td>
<td>-p</td>
<td>password for the certificate</td>
</tr>
<tr>
<td>-l</td>
<td>-l</td>
<td>length of the key</td>
</tr>
</tbody>
</table>

### Example
```
trac renew_p12 -s mygateway.domain.com -f "mycert.p12" -p mypass
```

## set_proxy_settings

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Args</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m</td>
<td>-m</td>
<td>one of no_proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- no_proxy - To disable proxy setting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- auto - To take proxy settings from the Internet Explorer LAN Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- manual - To set the proxy address (i.e. hostname and port)</td>
</tr>
<tr>
<td>-h</td>
<td>-h</td>
<td>hostname and port of the proxy</td>
</tr>
<tr>
<td>-p</td>
<td>-p</td>
<td>This can be set only when the proxy mode is manual</td>
</tr>
<tr>
<td>-u</td>
<td>-u</td>
<td>username and password credentials</td>
</tr>
<tr>
<td>-P</td>
<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 -p 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
```

**Arguments**
none
Appendix B

Creating a DLL file to use with SAA

In This Appendix

OPSEC - Open Platform for Security 110
Overview of SAA 110
How Does SAA Work 110
Summary of OPSEC API Functions 111

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.</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></td>
<td>Required for Ver 2</td>
<td></td>
</tr>
<tr>
<td>RegisterAgent or</td>
<td>RegisterAgent - Ver 1</td>
<td>Supplies the client with the functions required to work with the Authentication Agent.</td>
</tr>
<tr>
<td>RegisterAgentVer2</td>
<td>RegisterAgentVer2 - Ver 2</td>
<td></td>
</tr>
<tr>
<td>API Function</td>
<td>Version (Ver)</td>
<td>Summary of Functionality</td>
</tr>
<tr>
<td>------------------------------</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 UserNameAndPasswordVer2</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>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>
<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>
<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 <code>UserName</code> function.</td>
</tr>
<tr>
<td>usernameAndPassword</td>
<td>Out</td>
<td>The address of the Authentication Agent's <code>UserNameAndPassword</code> function.</td>
</tr>
<tr>
<td>Response</td>
<td>Out</td>
<td>The address of the Authentication Agent's <code>Response</code> function.</td>
</tr>
<tr>
<td>Terminate</td>
<td>Out</td>
<td>The address of the Authentication Agent's <code>Terminate</code> function.</td>
</tr>
<tr>
<td>Goingdown</td>
<td>Out</td>
<td>The address of the Authentication Agent's <code>GoingDown</code> 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/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>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</td>
<td>In - Length of the buffer allocated for response.</td>
</tr>
<tr>
<td></td>
<td>Out</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>
### Summary of OPSEC API Functions

#### AuthCompleted

**For Version 2**

The client calls `AuthCompleted` when authentication has completed. The Authentication Agent can notify the user of the authentication's results.

### AuthCompleted

**Prototype**

```c
int AuthCompleted(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 <code>Username</code> or <code>UsernameAndPassWord</code>.</td>
</tr>
<tr>
<td>status</td>
<td>In</td>
<td>The status of the authentication. One of these values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PLUGIN_DONE_SUCCESS - authentication was successful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PLUGIN_DONE_FAILED - authentication failed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PLUGIN_DONE - authentication has been cancelled for example, the password has expired or been erased.</td>
</tr>
<tr>
<td>message</td>
<td>In</td>
<td>The termination message, if provided by the authentication server.</td>
</tr>
</tbody>
</table>

**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>
<tbody>
<tr>
<td>context</td>
<td>In</td>
<td>The context as provided by Username or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UsernameAndPassWord.</td>
</tr>
</tbody>
</table>

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

```c
void InvalidateProcCB()
```

Arguments

There are no arguments.

Return Values

None.