Workspace Security

25 May 2026

REMOTE ACCESS VPN CLIENTS FOR WINDOWS

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

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

Certifications

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

Check Point Remote Access VPN Clients for Windows Administration Guide

For more about this release, see the Endpoint Security home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

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

Revision History

Date	Version	Comment
15 May 2026	All	Updated product names and product grouping to align with the new Check Point strategic pillars and portal navigation. No functional changes were made. Harmony Endpoint is now referred to as Check Point Endpoint Security.
27 February 2026	All	Added limitations for SDL. See *"Limitation" on page 66*.
17 January 2025	All	Corrected typos.
26 June 2024	All	Removed Secure Configuration Verification (SCV) topic. For SCV related information, see *Remote Access VPN Administration Guide* for your Security Gateway version.
09 August 2023	All	Updated: ■ *Example of a WindowsSecurityMonitor configuration*
02 July 2023	All	Updated: ■ *"Getting Started with Remote Access Clients" on page 22*
22 June 2023	All	Updated: ■ *"Endpoint Security VPN for Unattended Machines (ATMs)" on page 47*
09 May 2023	E87.30	Added: ■ *"Preserving Modified Default Settings After Upgrade" on page 55*

Table of Contents

Introduction to Remote Access Clients

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

The clients offered in this release are:

- **SmartEndpoint-managed Endpoint Security VPN** The Remote Access VPN blade as part of the Endpoint Security Suite connects users safely from their Endpoint Security-protected computer to corporate resources. The Compliance blade is managed from SmartEndpoint, and the Firewall can be managed from SmartConsole. Other Endpoint Security Software Blades that can be integrated include Media Encryption & Port Protection, Full Disk Encryption, Anti-Malware, and WebCheck.
- **SmartConsole-managed clients:**
  - **Endpoint Security VPN** - Incorporates Remote Access VPN with Desktop Security on one client. Check Point recommends this for managed endpoints that must have 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 safely 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 a primary targeted for non-managed machines.
  - **SecuRemote** - A secure, but small function IPsec VPN client, for small organizations that must have a small number of remote access clients.

To compare features, see the *Remote Access Clients Release Notes for your release*.

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.
- In-place upgrade from Endpoint Connect.

- Requires the IPsec VPN Software Blade on the Security Gateway, and an Endpoint Container license and Endpoint VPN Software Blade on the Security Management Server.

Check Point Mobile for Windows

- Enterprise Grade Remote Access Client.
- Secure Configuration Verification (SCV) is integrated with Windows Security Center to query the status of Anti-Virus, Windows updates, and other system components.
- Requires IPsec VPN and Mobile Access Software Blades on the Security 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 Security Gateway.
- It is a free client and it is not necessary to have more licenses.

Feature Overview

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

Primary Function	Description
Full IPSec VPN	Internet Key Exchange (version 1) support for secure authentication. A Virtual Private Network (VPN) provides a secured, encrypted connection on 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 apparently transparent because users can run an application or service that you do not block for the VPN. (Compare to SSL VPN, which operates through web applications only.)
Location Awareness	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 when the client exits the internal network.

Primary Function	Description
Multiple Login Options	Multiple login options for each gateway, with multi-factor authentication schemes.
Proxy Detection	Proxy servers between the client and the Security Gateway are automatically detected and authenticated to if necessary.
Dead Gateway Detection	If the client fails to receive an encrypted packet in a specified time interval, it sends a *tunnel test* packet to the Security Gateway. If the tunnel test packet is acknowledged, the Security Gateway is considered *on*. If some back-to-back tunnel test packets stay unacknowledged, the Security Gateway is considered inactive, or dead. You can configure this capability.
Multiple Entry Point	Provides a gateway High Availability and Load Sharing solution for VPN connections. For Remote Access Clients, in an environment with MEP, more than one Security Gateway protects and gives access to the same VPN domain. MEP allows the Remote Access Clients connect to the VPN from multiple gateways.
Secondary Connect	Gives access to multiple VPN gateways at the same time, to transparently connect users to distributed resources. Users log in one time to a selected site and receive transparent access to resources on different gateways.
Visitor Mode	If the firewall or network limits connections to ports 80 or 443, encrypted (IPSec) traffic between the client and the gateway is tunneled through a regular TCP connection.
NAT-T	**UDP Encapsulation of IPSec Traffic**. Remote Access Clients can connect seamlessly through devices that do not allow native IPSec traffic (such as firewall and access points).
Hub Mode	Increases security. It routes all traffic through the VPN and your Security Gateway. At the Security Gateway, the traffic is inspected for malicious content before being passed to the client, and you can control client connectivity.
VPN Tunneling	Increases connectivity performance. Encrypts only traffic targeted to the VPN tunnel, and allows users go more easily to sites where security is not an issue (such as public portals and search engines).

Primary Function	Description
Desktop Firewall	Endpoint Security VPN enforces a Desktop Firewall on SmartConsole-managed remote clients. The administrator defines the Desktop Security Policy in the form of a Rule Base. Rules can be assigned to specific user groups or all users; this permits the definition of flexible policies. SmartEndpoint-managed clients use the Endpoint Security Firewall blade.
Compliance Policy - Secure Configuration Verification (SCV)	SCV monitors the configuration of remote computers, to confirm that the configuration complies with organization Security Policy, and the Security Gateway blocks connectivity for computers that do not comply. It is available in Endpoint Security VPN and Check Point Mobile for Windows. In SmartEndpoint-managed clients, you can select to use SCV or the Endpoint Security Compliance blade.
Secure Domain Logon (SDL)	Establishes a VPN tunnel before a user logs in.
Certificate enrollment, renewal, and auto Renewal	Enrollment is the process of applying for, and receipt of, a certificate from a recognized Certificate Authority (CA), which here is Check Point's Internal CA. The system administrator creates a certificate and sends users the registration key. The client sends this key to Security Gateway, and in return receives the certificate.
Machine Authentication	Authentication with a machine certificate from the Windows system store.

Connectivity Features in Detail

Remote Access Clients support more connectivity features.

Feature	Description
Automatic Connectivity Detection	If the IPsec VPN network connection is lost, the client seamlessly reconnects without user intervention.
Roaming	If the IP address of a client changes, for example, if the client on a wireless connection physically connects to a LAN that is not part of the VPN domain, interface roaming maintains the logical connection.

Feature	Description
Multiple Sites	Remote Access users can configure many gateways to connect to the VPN. If you have multiple VPN gateways, users can attempt to connect to a different gateway if the previous one is down or overloaded.
Dialup Support	Endpoint Security VPN supports dial-up connections, useful where a network is not detected.
Hotspot Detection and Registration	Automatically detects hotspots that prevent the client system from establishing a VPN tunnel. Opens a mini-browser to allow the user to register to the hotspot and connect to the VPN gateway.
Office Mode	Allows a remote client appear to the local network as if it is uses a local IP address. This is not supported on SecuRemote.
Extended DHCP Parameters	When you use 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.
Machine Idleness	Disconnects the VPN tunnel if the computer becomes inactive (because of lock or sleep) for a specified duration.
Keep-alive	Send keep-alive messages from the client to the VPN gateway to maintain the VPN tunnel.
VPN Connectivity to VPN-1 VSX	Terminate VPN tunnel at Check Point VSX gateways.
Split DNS	Support multiple DNS servers.
DHCP Automatic Lease Renewal	Automatically renew IP addresses obtained from DHCP servers
Smart Card Removal Detection	If the Smart Card is removed from the PC, the VPN tunnel is closed.

Deployment Features

Feature	Description
Automatic Client Upgrade from the Security Gateway	Clients can automatically receive an upgrade package when they connect to the Security Gateway. For SmartConsole-managed clients only.
Pre-configured Client Packaging	You can create a default client installation package for easy provisioning.
Localization	Many supported languages.
Creating a Site from a Link	When the user clicks the link, the site is automatically created in the user's client.

General Features

Feature	Description
Post Connect Scripts	Run a script on client computers after a connection to the Security Gateway is established.
Post Disconnect Scripts	The post disconnect feature allows you to run a script on client computers after disconnection is established.

Supported Algorithms and Protocols

These algorithms are supported by Remote Access Clients to use with IKE:

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

These transport protocols are supported by Remote Access Clients:

- NAT traversal with UDP encapsulation, with allocated port set to **UDP VPN1_IPSEC_ encapsulation**.
- Visitor Mode through TCP connection with pre-configured port. By default, port 443.

Topology Architecture

Remote Access Clients Selective Routing allow you to configure 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**.
2. Select **Topology** to show the topology window.
3. Click **Set domain for Remote Access Community**.
4. Click **Set**.
5. From the drop down menu, select the object to represent the Remote Access VPN domain.
6. Click **OK**.

Encryption Domains

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

Scenario 1: Dedicated Encryption Domain

Component	Connects To
Gateway of Site 1	■ Gateway of Site 2 in Site-to-Site VPN ■ Remote Access Clients, as their VPN gateway
Gateway of Site 2	Gateway of Site 1 in Site-to-Site VPN
Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 2
Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 1
Remote Access Clients	■ Gateway of Site 1 through encrypted VPN ■ Permitted servers (3) ■ Note - cannot connect to denied servers (4)

Scenario 2: Access to External Encryption Domain

Component	Connects To
Gateway of Site 1	■ Gateway of Site 2 in Site-to-Site VPN ■ Remote Access Clients, as their VPN gateway ■ Relays clients to servers in other site's encryption domain (4) through VPN
Gateway of Site 2	Gateway of Site 1 in Site-to-Site VPN
Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 2
Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 1
Remote Access Clients	■ Gateway of Site 1 through encrypted VPN ■ Permitted servers (3 and 4) Note - Clients can reach servers of two sites with one authentication session, and their activity in both sites is logged

External Resources in Encryption Domain

Component	Connects To
Gateway of Site 1	■ Remote Access Clients , as their VPN gateway (5) ■ External resource (4) ■ Redirects clients (5) to external resource (4)
Remote Access Encryption Domain	■ Encrypted domain of Security Gateway (1) that includes an external resource
Servers in Encryption Domain	■ External resource
External (Internet or DMZ) resource in Encryption Domain	■ Server in Encryption Domain ■ Remote Access Clients if the Security Gateway redirects

Component	Connects To
Remote Access Clients	■ Gateway of Site 1 through encrypted VPN ■ Permitted servers (3) ■ External resource (4), through Security Gateway redirect

Getting Started with Remote Access Clients

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

Gateway Side Configuration

Before a user can connect to the Security Gateway with a Check Point Remote Access VPN client, the system administrator must configure these settings:

1. Security Gateway Configuration: Configure the Security Gateway to allow Remote Access VPN connections. Configure the necessary VPN policies, authentication methods, and access control rules for the Security Gateway.
2. VPN Server Address: Provide the server address or hostname of the VPN Gateway to users. Users need this information to connect to the correct VPN Gateway.
3. Authentication Method: Specify the authentication method for the Remote Access VPN client to use. Give users the necessary credentials or certificates. Common authentication methods:
    - username/password authentication
    - certificate-based authentication
    - multi-factor authentication
4. VPN Client Configuration File: You can preconfigure Remote Access VPN client settings in a configuration file that you provide to users. Users can import this file into the Remote Access VPN client to make configuration easier. Examples of settings you can predefine in the configuration file:
    - encryption algorithms
    - DNS settings
    - split tunneling options
5. Network Access Permissions: Define the network resources and permissions available to users connected through VPN. Specify which subnets, servers, applications, or servers users can access when they connect to the VPN Gateway.

For more information, see the *Remote Access VPN Administration Guide* for your version.

Simple Installation

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

To install Remote Access clients:

1. Download the MSI package and run 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. For versions before E86.60, confirm a destination folder.
6. Confirm that the installation should start.
7. Click **Finish**.

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

Also, see the Endpoint Security Clients for Windows User Guide.

Remote Access Clients Client Icon

The client icon shows the status of the client.

SmartConsole-managed:

Icon	Status
	Disconnected
	Connecting
	Connected
	Encryption (encrypted data is being sent or received on the VPN)
	There is an issue that requires users to take action.

SmartEndpoint-managed:

Icon	Status
	Disconnected
	Connecting
	Connected
	Connected but idle
	There is an issue that requires users to take action.

Helping Users Create a Site

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

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

Preparing the Gateway Fingerprint

Before users define a site that leads to the Security Gateway, prepare the fingerprint of the Security Gateway.

Users may get a warning that the client cannot identify the Security Gateway and that they should verify the fingerprint.

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

The Security Gateway Fingerprint can be prepared using either SmartConsole or the legacy SmartDashboard interface.

To prepare the Security Gateway Fingerprint from SmartConsole:

1. Open SmartConsole.
2. From the **Objects** dropdown, click **More object types** > **Server** > **New Trusted CA**.
3. In the **Certificate Authority Properties** window, select the **OPSEC PKI** tab.
4. In the **Certificate** field, click **View** to display the certificate details, and copy the SHA Fingerprint.

(Optional) To prepare the Security Gateway fingerprint from the legacy SmartDashboard:

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

To open the legacy SmartDashboard from SmartConsole:

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

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 Security Gateway.

   If a DNS server is configured and the client is within the internal network, the client detects the VPN site automatically.
3. The wizard shows the progress while the Client resolves the site name or address to the actual Security Gateway. A message shows:
   ```
   This may take several minutes, depending on the speed of your
   network connection.
   ```
4. If users see the certificate warning, make sure they check the fingerprint of the Security Gateway:

a. Compare the site fingerprint with the SIC fingerprint on the Security Gateway.

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

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

5. The wizard shows the authentication method window or **Login Option Selection** window.

   The options shown here depend on the method or methods you configure for the Security Gateway. If you configure multiple login options for a Security Gateway, users can select from multiple options.

6. The user selects an option and clicks **Next**.

7. If additional authentication factors are required, more windows open until the required authentication criteria are satisfied.

   For example:

   - If **Certificate**, the user selects **PKCS#12** or **CAPI** (make sure the user knows which to select), and clicks **Next**.
   - If **SecurID**, the user selects the type, and clicks **Next.**
   - If **Secure Authentication API (SAA)**, the user selects that and a new page opens to select the type of SAA and the DLL file. If a DLL file is already configured for the site, users do not have to select a file. Then click **Next**.

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

   If the user clicks **Yes**, the client connects to the Security 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**.

OR

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

Creating a Site from a Link

It may not be easy for a user to create a new site using the Site Wizard. Instead, you can email a link to users. When the user clicks the link, the site is automatically created in the user's client.

An example of a link that you can send to users:

```
cpvpn:///?host=192.0.2.198&auth=username-password
```

The link must be a clickable hyperlink, and the Remote Access client must run on the user's Windows computer.

Starting from R80.10, you can only create a site from a link when *"Feature Overview" on page 14* are not configured for the Security Gateway.

Link Syntax

```
cpvpn:///?host=<host>&auth=<auth_method>[&regKey=<cert_reg_key>]
[&fingerprint=<fingerprint>][&displayName=<displayName>]
```

Note - The syntax is case sensitive..

Parameters

Value	Description
<host>	Gateway IPv4 address or hostname. **Mandatory**.
<auth_method>	Authentication method. **Mandatory**. Must be one of these: ■ `username-password` ■ `certificate` (For a CAPI certificate) ■ `p12-certificate` ■ `challenge-response` ■ `securIDKeyFob` ■ `securIDPinPad` ■ `SoftID`
<cert_reg_key>	**Optional**. The registration key for the user's CAPI certificate. Not available for a P12 certificate. Add it if you want the Internal Certificate Authority to allocate a certificate automatically after the user creates the site (*"Feature Overview" on page 14*).

Value	Description
<fingerprint>	**Optional**: If you do not add this to the link, users are asked to approve the fingerprint the first time that they connect to the Gateway. Use the "+" character between the groups of characters in the fingerprint. For example: `GENE+RUN+HAND+JAY+HOOF+RAN+JILL+GRID+DARE+OATH+NICK+MIGO`
<displayName>	**Optional**: If you do not add this to the link, then the `<host>` is the display name for users. Spaces are not supported.

Link Examples

- `cpvpn:///?host=192.0.2.198&auth=certificate&regKey=27391-wbtx8d&fingerprint=LOY+LUSH+CANT+LOFT+LOB+TUCK+FAN+ALVA+MOW+AVER+A+SWAM`
- `cpvpn:///?host=192.0.2.198&auth=username-password`
- `cpvpn:///?host=192.0.2.198&auth=username-password&fingerprint=LOY+LUSH+CANT+LOFT+LOB+TUCK+FAN+ALVA+MOW+AVER+A+SWAM`

Changing the Login Option Settings

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

To select a different login option for authentication:

1. Open the **Authentication** tab of the client settings in one of these ways:
   - From the **Connect** window, click the link at the bottom of the window to **Change Login Option Settings**.

     The **Authentication** tab of the client settings opens.
   - From the desktop, right-click the client icon and select **VPN Options**.
     - The **Options** window opens.
     - In the **Sites** tab click **Properties**.
     - Click the **Authentication** tab.
2. Select a **login option**.

Under the login option are the factor or factors and the options available for those factors, such as a certificate type for **Certificate Authentication.**

3. If necessary, to activate a certificate, click **Import**, **Renew**, or **Enroll** and follow the on-screen instructions.
4. Click **OK**.

Helping Users with Basic Client Operations

Users can do basic client operations from the client icon.

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

To quickly connect to last active site, the user can double-click the client icon.

For other operations, the user can click the icon and select a command.

Command	Function
Connect	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.
Connect to	Opens the main connection window.
VPN Options	Opens the **Options** window to set a proxy server, choose interface language, enable Secure Domain Logon, collect logs, and select an SAA DLL file. In SmartConsole-managed only.
Shutdown Client	Closes the Client - In SmartConsole-managed only. 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.

For more VPN options in SmartEndpoint-managed clients:

1. Right-click the client icon and select **Display Overview**.
2. Click Remote Access VPN Blade.
3. Click one of the links for more options:

- **Manage connection details** - See details of your connection.
- **Manage settings** - Manage sites and Advanced VPN settings.
- **Register to hotspot** - Register to a hotspot to connect to the VPN from a hotspot.

Setting Up Remote Access Clients

Workflow for Deploying Clients

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

See sk67820 for the requirements for your environment

The initial workflow includes:.

1. Configure the Security Gateway that clients connect to.
2. Download a client package and edit the package, if necessary.

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

   a. **SmartEndpoint-managed Remote Access VPN** - Use the *"Creating Installation Package with VPN Configuration Utility" on page 36*.

   b. **SmartConsole-managed Remote Access Clients** - You can use these tools to edit the client MSI:

      - *"Creating Installation Package with VPN Configuration Utility" on page 36*.
      - Client application in Administration Mode.
      - CPMSI Tool with *"Editing an MSI Package with CLI" on page 39*
3. Distribute the package.
   - Through GPO or email, using the MSI file.
   - Distribute an upgrade automatically from the Security Gateway, using the TRAC.cab file. This is only for users who are upgrading from a previous version. You cannot edit the file before you distribute it.

Required Gateway Settings

You must configure one or more Security Gateways to work with Remote Access clients. These procedures are necessary for Remote Access clients operations.

For more information about the options in the procedures, see the Remote Access VPN Administration Guide for your Security Gateway version.

Configuring a Policy Server

The Policy Server functionality in a Security 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 SmartConsole, open the Security Gateway that will serve as the Policy Server.
2. Enable Policy Server functionality: In **General Properties** > **Network Security** tab, select **IPsec VPN** and **Policy Server**.
3. From the Security Gateway Properties, select **Other** > **Legacy Authentication**.
4. In the **Policy Server** area, from the **Users** list, select an existing user group of remote access clients.
5. Users that authenticate to the Security Gateway must belong to this group.
6. Click **OK**.

Configuring Logs on the Client

When logs are enabled, the client has two logging modes:

- Basic (default behavior)
- Extended

Basic mode filters very common logs which are mostly traffic related. In addition, it excludes log records with specific and configurable topics.

A default list of excluded topics is configured in `trac.defaults` configuration file.

Extended mode writes all log records to the client log files.

To disable logs altogether. clear the **Enable logging** checkbox in the Advanced tab below **VPN Options**.

Configuring VPN Settings

To configure the required Remote Access VPN settings:

1. In SmartConsole > **Security Policies** tab, right click the Security Gateway and select **Edit**.

   The **Check Point Gateway** window opens.

2. Enable VPN functionality: In the **General Properties** page, in the **Network Security** tab, select the **IPSec VPN** blade.

   Note - This enables all IPsec VPN functionality.

3. Add the Security Gateway to the **Remote Access VPN** community:
   a. From the Security Gateway Properties tree, click **IPsec VPN.**
   b. Under **This Security Gateway Participates in the following VPN Communities**, click **Add**.
   c. In the window that opens, select **Remote Access**.
   d. Click **OK**.
4. Set the VPN domain for the Remote Access community:
   a. From the Security Gateway Properties tree, select **Network Management** > **VPN Domain**.
   b. Click **Set domain for Remote Access Community**.
   c. In the window that opens, select the **Remote Access** VPN Community and click **Set**.
   d. In the window that opens, select a VPN Domain and click **OK**, or click **New** and define a VPN domain.
   e. Click **OK**.
5. Configure **Visitor Mode**:
   a. From the Security Gateway Properties tree, select **VPN Clients** > **Remote Access**.
   b. Select **Support Visitor Mode** and leave **All Interfaces** selected.
   c. Optional: Choose the Visitor Mode **Service**, which defines the protocol and port of Endpoint Security VPN connections to the Security Gateway.
6. Configure **Office Mode**:
   a. From the Security Gateway Properties tree, select **Office Mode**.
   b. Select an option: **Offer Office Mode to group** or **Allow Office Mode to all users**.
   c. Select an **Office Mode Method**.
   d. Click **OK**.

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

To add Remote Access Clients users to the VPN Community:

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

To configure encryption for the VPN:

1. From the SmartConsole menu, select **Global Properties**.
2. Select **Remote Access** > **VPN - Authentication and Encryption**.
3. In **Encryption Algorithms**, click **Edit**.
   - In **Support encryption algorithms** - Make sure that at least one **AES** encryption algorithm is selected.
   - In **Use encryption algorithm** - Make sure that at least one **AES** encryption algorithm is selected.
4. Click **OK**.
5. Click **OK**.

Important - The client does not support DES algorithms. An AES algorithm *must* be selected.
You can enable support for DES algorithms, if you also enable support for at least one AES algorithm.

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 Security Gateway is the VPN router for clients. All connections that the client opens are passed through the Security Gateway, even connections to the Internet.

You can exclude local networks when Hub Mode is enabled.

Note - Hub mode is not supported in SecuRemote.

To enable Hub Mode:

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

Excluding Local Networks from Hub Mode

When **Exclude local networks** is enabled:

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

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

To exclude local networks when hub mode is enabled:

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

To exclude local networks from the client:

1. Open the Remote Access client.
2. Click **Site Properties** > **Settings** tab.
3. Select **Do not route traffic for local network to the Security Gateway**.
4. Click **OK**.

   The changes is applied the next time that the user connects.

Closing TCP Sessions

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

To close all TCP sessions on Windows clients:

1. Edit the **$FWDIR/conf/trac_client_1.ttm** file on the Security Gateway.
2. Change the values of the parameters to `true`:
   - `close_TCP_connections_on_VPN_connect`
   - `fail_VPN_connect_on_closing_TCP_Connections_failure`
3. Save changes.
4. Install policy on the Security Gateway.

Configuring Authentication Settings for Users

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

You can configure multiple login options for a Security Gateway, with multiple authentication factors for each login option. Users see the different login options available and select one.

For details, see the VPN Remote Access Administration Guide for your Security Gateway version.

Creating Installation Package with VPN Configuration Utility

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

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

The VPN Configuration Utility gives you these options:

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

Using the VPN Client Configuration Utility

If you use this tool to create an MSI for SmartEndpoint-managed deployments, you must distribute it with an exported package, and not with Automatic Software Deployment.

To edit an MSI client package with the VPN Client Configuration Utility:

1. Get the MSI file:
   - SmartEndpoint-managed - Export a package that includes Remote Access VPN from the SmartEndpoint.
   - SmartConsole-managed - Download the MSI from the Support Center.
2. Run **VPNConfig.exe.**

   The VPN Client Configuration Utility opens on the **General** tab.
3. Click **Browse** to select the location of the MSI.
4. Select the options and their values to include in the MSI:
   - **Secure Domain Logon** - To control whether the authentication credentials sent to the Domain Controller are sent through an encrypted channel.
   - **Fixed MAC** - To control whether to use fixed MAC address for Office Mode IP address allocation.

- **No Office Mode** - To control Office Mode support.
- **Replace trac.defaults file** - This file includes the default values for configuration attributes.
- **Replace trac.config file** - This file includes VPN Site configuration.

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

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

   Important:
   - If you selected to replace the `trac.config` file, then you have to provide the path for both `trac.config` and `trac.defaults` files.
   - If you selected to replace the `trac.config` and `trac.defaults` files, then you have to use the configuration files from the same version as the customized MSI package. For example, if you need to customize the MSI of E87.10, then use the `trac.config` and `trac.defaults` from E87.10.

6. **Optional:** Create a CAB file for Standalone VPN Client only.

   Select the **Save CAB as well (Standalone VPN Client only)** check box to create a `TRAC.cab` file to use for an upgrade with SmartEndpoint-managed client.

   - Create a `ver.ini` file with the correct build number. Make sure the build number is higher than the build number in the current ver.ini file (located in the Endpoint Client installation directory).
   - To upgrade using a customized `TRAC.cab` file, users need to use it together with *"Upgrading with a Customized Package" on page 46*.

7. **Optional:** Open the **Edit Files** tab.

   Add the desired files to the installation directory. For example, a script to use with *"Configuring Post Connect Scripts" on page 96*.

8. **Optional:** Open the **Advanced** tab.

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

9. Click **Save**.
10. Select the location where the new MSI will be saved.

Editing an MSI Package with CLI

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

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

Syntax

```
package-package-file-name>
```

```
[<-in|-out|-add|-overwrite|-overwrite|-copyout|-add_scv_plugin|-
remove_scv_plugin|-overwrite_scv_plugin> <filename>]
```

```
[-replace_config <true|false>] [-sdl_enable <true|false>] [-fixed_
mac <true|false>]
```

```
[-client_sub_type
<SecuRemote|CheckPointMobile|EndpointSecurityVpn|UserDecide>]
```

Parameters

Parameter	Description
-in	Add a file `<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`

Parameter	Description
-out	Remove a file <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 a file <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 a file <filename> with a new version of the file. It must be a file that was added.
-copyout	Save a file <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 Secure Domain Logon (SDL) Possible values: true or false ■ true - Secure Domain Logon (SDL) is enabled for the package. ■ false - Secure Domain Logon (SDL) is disabled for the package.

Parameter	Description
-fixed_mac	Possible values: `true` or `false` ■ `true` - The client will use fixed Office mode MAC addresses. ■ `false` - The client will not use fixed Office mode MAC addresses.
-client_sub_type	Default client type. Possible values: ■ `SecuRemote` ■ `CheckPointMobile` ■ `EndpointSecurityVpn` ■ `UserDecide`
	Notes - **DisconnectedPolicy.xml** is on client computers in: ■ Windows Vista and higher - `C:\Windows\System32\drivers` ■ Windows XP - `C:\Windows\System32` **LangPack1.xml**is on client computers in the installation directory: ■ 32 bit - `C:\Program Files\CheckPoint\Endpoint Connect` ■ 64 bit - `C:\Program Files (x86)\CheckPoint\Endpoint Connect`

Adding Initial Firewall Policy with CLI

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

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

- `DisconncetedPolicy.xml`
- `desktop_policy.ini`

Note - An initial firewall is only supported in a new Remote Access Clients installation..

To add the files required for an initial firewall, run:

```
cpmsi_tool -in DisconncetedPolicy.xml -overwrite desktop_policy.ini
```

Installing an MSI Package with CLI

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

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

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

Type of Installation	Command	Notes on Flags
Regular - Use this for a non-ATM installation. All prompts show. The Cancel button does not show so that users cannot stop the installation after it starts. If necessary, a restart prompt opens when the installation completes.	`\"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qb! INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect"`	**qb!** - Basic UI level
Silent - Use this for an ATM installation. User interface shows on the screen but users do not press anything. If necessary, the client automatically restarts.	`\"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qb-! INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect"`	**qb-!** No user interaction is required

Type of Installation	Command	Notes on Flags
No User Interface - All user interface is hidden.	`\"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qn INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect"`	**qn** - no UI

Distributing MSI Packages

You can distribute MSI files to users in different ways:

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

Users must have administrator privileges to install the MSI.

For all installation types, make sure users have whatever is needed for authentication. For example, if users authenticate with certificates, make sure they have the certificate file before connection. Make sure they know that they must not delete this file.

Some examples of client deployment options are:

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

Automatic Upgrade from the Security Gateway

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

The installation is downloaded automatically from the Security Gateway, and it installs automatically.

This is only for users who are upgrading from a previous version. You cannot edit the file before you distribute it.

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

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

Each package has these files:

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

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

Unattended (ATM) Clients

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

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

Distributing the Remote Access Clients from the Gateway

Follow these steps to automatically upgrade the Remote Access client when users connect to the Security Gateway.

Step 1: Create backup copies of the applicable files

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Create backup copies of these files:
   a. `cp -v $FWDIR/conf/extender/CSHELL/TRAC.cab{,_BKP}`
   b. `cp -v $FWDIR/conf/extender/CSHELL/trac_ver.txt{,_BKP}`

Step 2: Download the Remote Access Clients Automatic Upgrade file for your release

1. Go to sk117536 - Endpoint Security Home Page and navigate to the **Client Releases Information** section.
2. Identify your installed client version and click the row corresponding to your version.
3. In the **Release Home page** section, open the mentioned SK and navigate to the **Standalone Client Downloads** section.
4. From the **Remote Access VPN Clients (Automatic Upgrade file)** section, download the **.CAB* file and rename it from **.CAB* file to: *TRAC.cab*.
5. On your system:

a. Open the downloaded *TRAC.cab* file.

b. Open the *ver.ini* file.

c. Copy the build number and save it.

Step 3: Configure the Security Gateway / each Cluster Member

1. Transfer the downloaded *TRAC.cab* file to the Security Gateway / each Cluster Member to some directory (for example, */var/log/*).
2. On the Security Gateway / each Cluster Member, assign the required permissions to the *TRAC.cab* file:

   ```
   chmod -v 775 /var/log/TRAC.cab
   ```

3. On the Security Gateway / each Cluster Member, copy the *TRAC.cab* file to the required directory:

   ```
   cp -v /var/log/TRAC.cab $FWDIR/conf/extender/CSHELL/
   ```

4. On the Security Gateway / each Cluster Member, change the build number in the *trac_ver.txt* file:

   a. Edit the file:

      ```
      vi $FWDIR/conf/extender/CSHELL/trac_ver.txt
      ```

   b. Change the current build number to the build number you saw in the *ver.ini* file.

   c. Save the changes in the file and exit the editor.

Step 4: Configure the client upgrade mode

1. Connect with SmartConsole to the Management Server that manages the Security Gateway / Cluster.
2. In SmartConsole, click the **Menu** button > **Global properties**.
3. From the left tree, click **Remote Access** > **Endpoint Connect**.
4. In the section **Client upgrade mode**, select the applicable option:
   - **Ask user** (end-users must confirm the client upgrade)
   - **Always upgrade** (automatic client upgrade without asking end-users)
5. Click **OK**.

Step 5: In SmartConsole, install the policy on the Security Gateway / Cluster

Configuring Upgrades

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

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

To configure how to deploy changes to the client:

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

Upgrading with a Customized Package

You can create a customized MSI package and deploy it from the Security Gateway as part of the TRAC.cab file. For example, you can include a defined `trac.config` file and 3rd party SCV plugins.

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

To upgrade with a customized MSI:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Add `upgrade_accept_customized_packages` and set its value to `true`.
3. Create a Microsoft CAB file that contains:
   - Your MSI file renamed `TRAC.msi`
   - `ver.ini` with the correct build number

4. Sign the CAB file with a certificate that is trusted on the target computer in these local computer certificate stores:
   - The CA certificate must be trusted in the Trusted Root Certification Authorities store
   - The Publisher certificate (used to sign the CAB file) must be trusted in the local computer's Trusted Publishers store
5. Use the procedure in *"Distributing the Remote Access Clients from the Gateway" on page 44*.

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 *"Remote Access Clients Command Line" on page 106* 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.

If an unattended client gets an automatic upgrade from the Security 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 Security Gateway. Instead, upgrade attended and unattended clients with the applicable MSI file.

Configuring the client for ATMs

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

- Make sure that there is an application that uses the client API to start and monitor the connection.

  You can configure the client for **always-connect** (rather than the API). But we do not recommend this if you use **secondary connect**. If the primary tunnel disconnects and the machine reboots, a client in **always-connect** does not connect to the backup tunnel. It tries to connect to the primary tunnel.

  If you want always-connect and secondary connect, we recommend that you use a 3rd party code to switch to the secondary tunnel on failover.

- Make sure the ATM machine has a certificate in the CAPI, and that the client is configured for **automatic CAPI re-authentication**.

Administrators can configure username and password caching for ATM devices in the Windows registry. Credentials are saved encrypted in the registry per site. This feature does not depend on password caching. See *"Remote Access Clients Command Line" on page 106* for feature usage.

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

To enable automatic CAPI re-authentication:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Add these lines:

```
:automatic_capi_reauthentication (
:gateway (automatic_capi_reauthentication
:default (true)
)
)
```

3. Save the file.
4. Install policy.
5. Apply this configuration to all gateways.

Note - To learn more about the TTM file, see *"The Configuration File" on page 138*.

Configuring Username and Password caching for ATM machines

Configure username and password caching for ATM devices in the Windows Registry. Credentials are saved encrypted in the Windows Registry per VPN site. This feature does not depend on password caching. To enable the feature, change an attribute in the `trac.defaults` file: `save_cli_credentials_for_ATM` from the default value of `false` to `true`.

Note: This procedure is for an already installed ATM client, or when creating a deployment client package.

To configure username and password caching for ATM machines:

1. Stop the Endpoint Connect service in Windows Command Prompt by running the following command:

   ```
   C:\> trac stop
   ```

2. Browse to Endpoint Connect folder:

   On a 32-bit system:
   `C:\Program Files\CheckPoint\Endpoint Connect\trac`

   On a 64-bit system:
   `C:\Program Files (x86)\CheckPoint\Endpoint Connect\trac`

3. Backup the `trac.defaults` file.
4. Edit the `trac.defaults` file in a plain-text editor (for example Notepad).
5. Set the value of `save_cli_credentials_for_ATM` parameter to `true`:

   modify the line from

   ```
   save_cli_credentials_for_ATM STRING false GW_USER 0
   ```

   to

   ```
   save_cli_credentials_for_ATM STRING true GW_USER 0
   ```

6. Save changes and exit the text editor.
7. Start the Endpoint Connect service in Windows Command Prompt by running:

   ```
   C:\> trac start
   ```

   Note: The `save_cli_credentials_for_ATM` feature is not related to **Enable password caching** in the SmartConsole Global Properties (Remote Access > Endpoint Connect). You do not need to configure the Global Property for the first time to work

Saving the credentials for the VPN site configured with username-password authentication

1. Open a Windows command prompt as an administrator:

   In the Windows search, type **cmd** > In the search results, right-click **cmd.exe** > Select **Run as administrator**
   Changes to the Windows Registry do not take effect unless you run `cmd.exe` as an administrator. It is not enough to be logged to Windows in as administrator.

2. Browse to Endpoint Connect folder:

   On a 32-bit system
   `C:\Program Files\CheckPoint\Endpoint Connect\trac`

   On a 64-bit system
   `C:\Program Files (x86)\CheckPoint\Endpoint Connect\trac`

3. Save the username and password for an existing VPN site by running the command:

   ```
   C:\> trac userpass -s <sitename> -u <username> -p <password>
   ```

4. Make sure that the credentials are cached (encrypted) in the Windows registry:

   a. Start Windows built-in Registry Editor:
   Start menu > In the search field, type **regedit** and click Enter.

   b. Check the new keys are added for the VPN site:

   ```
   HKEY_LOCAL_
   MACHINE\SOFTWARE\Wow6432Node\CheckPoint\TRAC\sites\"Site_
   Name/Site_IP_Address"
   ```

Configuring Reauthentication Time

Configure the reauthentication time in SmartConsole or SmartConsole.

To configuring the reauthentication time:

1. In SmartConsole, click **Menu**.
2. Click **Global Properties**.
3. Click **Remote Access** > **Endpoint Connect**.
4. Configure the number of minutes **Re-authenticate user every**.
5. Click **OK**.
6. Install the policy on the Security Gateway or Cluster.

Configuring the Client Package

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

To configure the package for ATMs:

1. Install non-ATM Endpoint Security VPN on a client machine.
2. Create a site.

   For each Security Gateway on the site, users have to connect and approve the fingerprint.

   Note - The last connected Security Gateway will be defined as the primary gateway in the generated package deployment.
3. Go to `c:\program files\checkpoint\endpoint` and run `AdminMode.bat`.
4. Go to **VPN Options** > **Administration** tab.
5. In the **Input MSI Package path** field, enter the path name of **CheckPointEndpointSecurityForATM.msi**.
6. Select **Replace user's configuration when upgrading**.
7. In **Select a product**, select **Endpoint Security VPN**.
8. Click **Generate**.
9. Save the MSI to the local disk.
10. Enable **No Office Mode** on the MSI:
    a. At the Windows command prompt, `go to c:\program files\checkpoint\endpoint`.
    b. Run this command:

    ```
    cpmsi_tool.exe CheckPointEndpointSecurityForATM.msi-NO_OFFICE_MODE1
    ```

Deploying the Client Package Manually

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

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

To upgrade the client manually:

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

Using DNS for Automatic Site Detection

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

This DNS query:

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

To configure automatic DNS site detection:

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

Property	Value
Service	CHECKPOINT_RA_
Protocol	_tcp
Port number	443
Host offering this service	Name of the Security Gateway as used in the DNS record

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 *"Using the Update Configuration Tool" on the next page*.

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

In versions E87.20 and lower:

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

Starting from version E87.30:

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

Parameters

Parameter	Description
old `trac.config` file name and path	The path on the user's machine to the temporary location where they put the old `trac.config` file. For example, `"C:\Windows\Temp\trac.config"`.
product directory	The installation directory of the Remote Access Client on the user's machine. For example, `"C:\Program Files\CheckPoint\Endpoint Connect\"`.

Using the Update Configuration Tool

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

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

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

1. Stop the 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:
   - In versions lower than E87.30: `update_config_tool "C:\Windows\Temp\trac.config" "C:\Program Files\CheckPoint\Endpoint Connect\"`

- Starting from version E87.30: `update_config_tool/config "C:\Windows\Temp\trac.config" "C:\Program Files\CheckPoint\Endpoint Connect\"`

5. Start the Remote Access clients services from the CLI:

```
net start tracsrvwrapper
```

Preserving Modified Default Settings After Upgrade

By default, when you upgrade a Remote Access VPN client version E87.30 or higher, changes to default settings in the *trac.defaults* file made by an administrator or a user are preserved.

For example, in the *trac.defaults* file of a Remote Access VPN client version E87.30, a user changed the value of the *machine_tunnel_site* parameter to the name of a site for machine-only authentication (example: *MachineSite*). The default value of this parameter is "" (empty string). After an upgrade, the *machine_tunnel_site* parameter retains the value *MachineSite*.

Upgrading Remote Access VPN Client Without Preserving Modified Default Settings

Starting from E87.30, to upgrade a Remote Access VPN client **without** preserving modified default settings, you must run the installation package from Windows Command Prompt and pass the value of a parameter in the package.

To upgrade the Standalone Remote Access VPN client without preserving modified default settings:

1. Open Windows Command Prompt in the directory where the upgrade package (*CheckPointVPN.msi*) is located.
2. Run:

```
CheckPointVPN.msi DISABLE_DEFAULTS_MERGE=1
```

To upgrade the Endpoint Security Client without preserving modified default settings for Remote Access VPN:

1. Open Windows Command Prompt in the directory where the upgrade package (*EPS.msi*) is located.
2. Run:

```
EPC_DISABLE_DEFAULTS_MERGE=1
```

Known Limitations

- Preservation of modified default settings is disabled if you use the VPN Configuration Tool to replace the *trac.defaults* file in a customized upgrade package

Third-Party Anti-Virus Scanning Exclusion

When you install Endpoint Security VPN Client for Windows on a device that already has third-party anti-virus software installed, it is recommended to exclude certain files from the anti-virus scans.

To add exclusions to the Anti-Virus scan:

Exclude these folders:

- `C:\Program Files\CheckPoint\`
- `C:\Program Files (x86)\CheckPoint\`
- `C:\ProgramData\Check Point\`
- `C:\ProgramData\CheckPoint\`

Exclude these Window registries:

- `HKEY_LOCAL_MACHINE\SOFTWARE\CheckPoint\`
- `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\CheckPoint\`
- `HKEY_CURRENT_USER\SOFTWARE\CheckPoint\`

Exclude these drivers:

The drivers in `C:\Windows\System32\drivers\` must only be excluded if the Anti-Virus causes an issue with them.

- Path - `C:\Windows\System32\drivers\`
- PowerShell command to list the files in: `C:\Windows\System32\drivers\` that belong to Check Point:

  ```
  cd C:\Windows\System32\drivers\

  Get-ChildItem | Format-List -Property VersionInfo
  ```

Configuring Client Features

Intel Smart Connect Technology

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

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

To enable automatic Intel Smart Connect Technology:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Add these lines:

```
:enable_intel_aoac (
 :gateway (enable_intel_aoac
 :default (true)
 )
)
```

3. Save the file.
4. Install policy.

HotSpot Registration

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

To configure any port for HotSpot registration:

1. Connect with the Database Tool (GuiDBEdit Tool) to the Management Server.
2. On the **Tables** tab, open **Global Properties > properties > firewall_properties > registration > ports**.
3. Remove the pre-defined ports.
4. Add a new element that uses the string value: `<any_port>`.
5. Click **File > Save all**.

6. Connect with SmartConsole to the Management Server.
7. Open **Global Properties > Remote Access > Hot Spot/Hotel Registration**.

   The **Ports to be opened during registration** field now shows **<any_port>**.

   Note - The client must also be able to register to the *"hotspot_reg" on page 116*.

Hotspot Registration with Default Browser

You can register to hotspots with the computer's default browser instead of the client's embedded browser.

To enable default browser launch:

1. Go to the **Endpoint Connect** Program folder:
   - 64-bit systems - `%programfiles(x86)%\CheckPoint\Endpoint Connect\`
   - 32-bit systems - `%programfiles%\CheckPoint\Endpoint Connect\`

   For clients that are part of the Endpoint Security suite, the end of the path is `CheckPoint\Endpoint Security\Endpoint Connect`.
2. Edit the `trac.defaults` file in a plain-text editor like Notepad.
3. Locate the `open_default_browser_for_hotspot` parameter and change its value from **false** to **true**.
4. Save the file.
5. Open the Command Prompt as Administrator and run:

   ```
   > net stop TracSrvWrapper
   > net start TracSrvWrapper
   ```

To disable default browser launch:

1. Go to:
   - 64-bit systems - `%programfiles(x86)%\CheckPoint\Endpoint Connect\`
   - 32-bit systems - `%programfiles%\CheckPoint\Endpoint Connect\`
2. Edit the `trac.defaults` file in a plain-text editor like Notepad.
3. Locate the `open_default_browser_for_hotspot` parameter and change its value from **true** to **false**.
4. Save the file.

5. Open the Command Prompt as Administrator and run:

```
> net stop TracSrvWrapper
> net start TracSrvWrapper
```

Managing Desktop Firewalls

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

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 Security Gateway.

Endpoint Security VPN downloads the first policy from the Security 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 Security Gateway and downloads its policy. Endpoint Security VPN enforces the policy: accepts, encrypts, or drops connections, depending on their source, destination, and service.

Endpoint Security VPN Desktop Policy Architecture

1	Security Management Server	Manages all policies.
2	Gateway	Firewall of LAN, holds Desktop Security Policy and TTM configuration.
3	Endpoint Security VPN client	Gets Desktop Security Policy from Security Gateway and enforces policy on client computer.

Choose a Firewall Policy to Enforce

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

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

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

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

Action	Description
Enforce the above Firewall policy	Use the Endpoint Security Firewall Policy Rules
Enforce Desktop Policy from SmartConsole	Use the Desktop Policy from SmartConsole

3. Install Policy.
4. Restart all computers included in the rule.

Rules

The Desktop Security Policy has Inbound and Outbound rules.

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

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

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

Implied Rules

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

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

User Granularity

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

- **Locations** - Set rules to be implemented by physical location. For example, a user with a laptop in the office building will have a less restrictive policy than when the same user on the same laptop connects from a public wireless access point.
- **User Groups** - Set rules to be implemented for some users and not others. For example, define restrictive rules for most users, but give system administrators more access privileges.

  Rules are applied to user groups, not individual users. Endpoint Security VPN does not inherently identify user groups, so it must obtain group definitions from the Security Gateway. The Security 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 Security Gateway, the client enforces a *default policy*. This policy is enforced until Endpoint Security VPN connects to the Security Gateway and enforces an updated personalized policy.

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

Configuring a Desktop Firewall Policy

Before you begin, make sure that you enabled the Policy Server on the Security Gateway. See *"Configuring a Policy Server" on page 32*.

Desktop Security Policy

To create a Desktop Security Policy with Security Management:

1. In SmartConsole, **Security Policies**, under **Access Control**, right-click **Policy** and select **Edit Policy**.
2. In the **Policy Types** area, select **Desktop Security**.
3. Click **OK**.

   Desktop shows in list under **Access Control**.
4. Click **Desktop** and click **Open Desktop Policy in SmartConsole**.

   A SmartConsole window opens.
5. In SmartConsole, open the **Desktop** tab.
6. Configure the rules: Click in the **Inbound Rules** or **Outbound Rules** section and click an **Add Rule** icon to add a new rule.

   For each rule, you can include users for whom the rule applies.

   - In inbound rules, **Desktop** (Endpoint Security VPN) is the destination.
   - In outbound rules, **Desktop** is the source.
7. Save the changes in SmartConsole.
8. In SmartConsole, click **Install Policy.**
9. In the **Install Policy** window:
   a. Select **Desktop Security**.
   b. Select the gateways that are configured to handle Endpoint Security VPN traffic.
   c. Click **Install**.

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.

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

Planning Desktop Security Policy

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

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

Location-Based Policies

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

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

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

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

Location Awareness Policy Configuration

This release introduces two new properties in client configuration:

- disconnected_in_house_fw_policy_enabled - Defines if the feature is enabled or disabled.

  Possible values are:

  - true - enabled
  - false - disabled **(default)**

- disconnected_in_house_fw_policy_mode - Defines which policy will be enforced after Location Awareness detection.

  Possible values are:

  - encrypt_to_allow - Connected policy will be enforced, based on last connected user. Encrypt rules will be transformed to Allow rules **(default)**.
  - any_any_allow - "Any - Any - Allow" will be enforced.

To enable Location Awareness for desktop firewall:

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

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

3. Save the file and install the policy.

To configure the location based policy:

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

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

3. Save the file and install the policy.

Note - It is highly recommended to configure default values for these properties in `trac_client_1.ttm` for all gateways.

Allow/Block IPv6 Traffic

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

To block IPv6 traffic to the client:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Add these lines:

```
:allow_ipv6 (
 :gateway (allow_ipv6
 :default (false)
 )
)
```

3. Save the file.
4. Install policy.

Logs and Alerts

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

- 32-bit systems - **C:\Program Files\CheckPoint\Endpoint Connect\trac_fwpktlog.log**
- 64-bit systems - **C:\Program Files(x86)\CheckPoint\Endpoint Connect\trac_fwpktlog.log**

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

Wireless Hotspot/Hotel Registration

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

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

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

A proxy might be required.

Letting Users Disable the Firewall

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

If this option is enabled, when users right-click the Remote Access Clients icon, they can select **Disable Security Policy**.

To change the Allow disable firewall setting:

1. Edit the $`FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Find the line `:allow_disable_firewall` and set the applicable value:
   - **true** - Users can disable their firewall policy.
   - **false**- Users do not have the option to disable their firewall policy.
   - **client_decide** - Takes the value from a file on the client machine
3. Save the file.
4. 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.

Limitation

Hotspot registration is not supported with SDL.

Configuring SDL

To enable SDL:

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

SDL for SmartConsole-Managed Clients

To create an SDL-enabled client:

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

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

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

To help users enable SDL on a client:

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

To enable Remote Access Clients to use SDL:

1. On SmartConsole, 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 `CachedLogonsCount`, with the valid value range of 0 to 50.

   The value of the key is the number of previous logon attempts that a server will cache.

   A value of 0 disables logon caching. A value over 50 will only cache 50 logon attempts.

SDL in Windows

There are different SDL modes for Windows:

- Explicit
- Implicit

Using Explicit Mode

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

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

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

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

Using Implicit Mode

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

The user cannot authenticate to the domain controller over a VPN, but the client can receive a Group Policy and logon scripts. The Windows operating system authenticates to the domain controller using the cache. To use Implicit mode the end user must

1. Enable Windows *"Configuring Windows Cached Credentials" on the previous page*.
2. Have one successful login to Windows cached in the registry.

Note - Implicit mode SDL is not invoked with smart card logon to Windows.

Disable or Enable SDL on Internal Network

By default, the Remote Access client automatically disables Secure Domain Login (SDL) when the client detects one of these conditions:

- It is connected to an internal network.
- It is connected to the VPN domain.
- There is no network.

Until the client gets a response from the location awareness feature, the decision is based on the fact that the client has an IP address in the VPN Domain.

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

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Search for: `ignore_sdl_in_encdomain`.

   If the property does not exist, create it.
3. Set the required value according to this table:

Value	Meaning
`true`	The **Connect** window of the Remote Access client does not appear when the client detects one of these conditions: ■ It is connected to an internal network. ■ It is connected to the VPN domain. ■ There is no network. This is the default value.
`false`	The **Connect** window of the Remote Access client always appears.

1. Save the file.
2. Install policy on the Security Gateway.

Disable Implicit SDL

To disable Implicit SDL when SDL is enabled:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the VPN gateway.
2. Add these lines if they do not exist:

```
:implicit_sdl_enabled (
    :gateway (
        :default (<value>)
    )
)
```

Where <value> can be:

- **true -** Implicit SDL is enabled
- **false -** Implicit SDL is disabled

3. Save the file.
4. Install policy.
5. Apply this configuration to all applicable Security Gateways.

Multiple Entry Point (MEP)

Multiple Entry Point (MEP) gives high availability and load sharing to VPN connections from Remote Access Clients to the internal network of the organization.

A Security Gateway is one point of entry to the internal network. If the Security Gateway becomes unavailable, the internal network is also unavailable. A Check Point MEP environment has two or more Security Gateways for the same VPN domain to give remote users uninterrupted access.

MEP 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 Automatic MEP, gateways must have the same management server.
- There is no state synchronization in MEP. If a Security Gateway fails, the current connection fails and one of the backup gateways picks up the *next* connection.
- Remote clients, not the Security Gateways, find the Security Gateway to use. To find the Security Gateway to use, the clients use a mechanism called Visitor Mode.

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 from Global Properties.
- **Manual** - You can edit the list of MEP Security Gateways in the Remote Access Clients TTM file.

To define MEP topology:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Search for: `automatic_mep_topology`
3. If you do not see this parameter, add it manually as shown here:

```
:automatic_mep_topology (
    :gateway (
        :map (
            :true (true)
            :false (false)
        )
        :default (true)
    )
)
```

4. Set the value of `:default` to:
   - `true` - for implicit configuration
   - `false` - for manual configuration
5. **For Manual MEP only**: Make sure that the value of `enable_gw_resolving` is `true`.

```
:enable_gw_resolving (
    :gateway (
        :default (true)
    )
)
```

6. Save the file.
7. Install the policy.

Implicit MEP

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

Before you start, make sure that **$FWDIR/conf/trac_client_1.ttm** on each Security Gateway has `automatic_mep_topology` property, and that property has the `:default` value of `true`:

```
:automatic_mep_topology (
    :gateway (
        :map (
            :true (true)
            :false (false)
        )
        :default (true)
    )
)
```

Configuring Implicit First to Respond

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

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

To configure First to Respond MEP:

1. Find out which gateways are in the VPN domain. In the VPN CLI, run:
   `vpn overlap_encdom`
2. Create a host group and assign all of these gateways to it.
3. In the **Properties** window of each Security 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 Security 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 Security Gateway. If the selected Security Gateway does not respond in the configured time, the first Security Gateway that responded gets the connection.

Configure the same grace period on each Security Gateway.

To give preference to the selected Security Gateway:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on each Security Gateway.
2. Find the `mep_prefer_chosen_gw_grace_period` parameter.
3. Set the required grace period in milliseconds.
4. Save the file.
5. Install the policy.

Configuring Implicit Load Distribution

To configure implicit MEP for random Security Gateway selection:

1. Click **Menu** > **Global Properties**.
2. Open the **VPN** > **Advanced** page.
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. In each Security Gateway network object, go to the **Network Management** > **VPN Domain** page, and select **Manually defined**.
   c. Select the group.
5. Click **OK**.
6. Install the Access Control Policy.

Configuring Implicit Primary-Backup

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

To configure the primary Security Gateway:

1. Open **Global Properties** window > **VPN** > **Advanced**, select **Enable Backup Gateway**.
2. In the Object Explorer, click **New** > **Network Group** and create a group of gateways to act as backup gateways.
3. Edit the Primary Security Gateway object and open the **IPsec VPN** page.
4. Select **Use Backup Gateways**, and select the group of backup gateways.

This Security Gateway is the primary Security Gateway for this VPN domain.

5. For each backup Security 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 Security 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 Security Gateway.

   b. In the backup network object, go to the **Network Management** > **VPN Domain** section, select **Manually defined**.

   c. Select the group.

6. Click **OK**.

7. Install the policy.

Manual MEP

For Manual MEP, the gateways do not have to belong to the same VPN domain. Configure the TTM file of each Security Gateway.

To configure the gateways for MEP:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Management Server.

2. Search for the `enable_gw_resolving` attribute:

```
:enable_gw_resolving (
    :gateway (
        :default (true)
    )
)
```

3. Make sure the attribute's default value is `true`.

4. Search for the `automatic_mep_topology` attribute, and make sure its value is `false`.

5. Manually add the `mep_mode` attribute with the required value:

```
:mep_mode (
    :gateway (
```

```
        :default (VALUE)
    )
)
```

Where VALUE is one of these:

- **first_to_respond**
- **primary_backup**
- **load_sharing**
- **dns_based -** Use this to configure *"Configuring Geo Cluster DNS Name Resolution" on the next page*.

6. Manually add the `ips_of_gws_in_mep` attribute with the required IP addresses:

```
:ips_of_gws_in_mep (
    :gateway (
        :default (<IP_Address_1>&#<IP_Address_2>&#...<IP_Address_
X>&#)
    )
)
```

These are the IP addresses the client should try.

- IP addresses are separated by an ampersand and hash symbol (`&#`)
- The last IP address from the list must also have the `&#` characters.

Example: `192.168.53.220&#192.168.53.133&#`

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 primary 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 SmartConsole, 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

To configure Geo Cluster DNS Name Resolution in Manual MEP mode:

1. In the `trac_client_1.ttm` configuration file, find `mep_mode`. If you do not see this parameter, add it as shown here:

```
:mep_mode (
    :gateway (
        :default (dns_based)
    )
)
```

2. Set the value of `:default` to `dns_based`.
3. Save and close the file.
4. Configure IP pool NAT or Hide NAT to manage return packets.

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 Security Gateway, without site-to-site communication. VPN tunnels and routing parameters are automatically taken from the network topology and destination server IP address.

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

For gateway requirements for Secondary Connect, see sk65312.

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 Security Gateway:

1. Make sure the Security Gateway has a server certificate that is signed by the internal Certificate Authority.
2. Edit the `$FWDIR/conf/trac_client_1.ttm` file on each Security Gateway.
3. Set the `:default` value of `automatic_mep_topology` to `true`.
4. Search for: `enable_secondary_connect`
5. 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)
)
)
```

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

Secondary Connect for Users

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

If their credentials are not cached, they might be prompted to authenticate again for a secondary connection.

Link Selection for Remote Access Clients

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

Configuring Link Selection for Remote Access

To configure Link Selection for Remote Access:

1. In SmartConsole, open the Security Gateway object properties.
2. Go to the **IPSec VPN > Link Selection** page.
3. Select the **Link Selection** method:
   - **Always use this IP address** - when a VPN peer tries to determine the IP address of the Security Gateway, it always uses the IP address specified here.

Main address	The main IP address of the Security Gateway, as specified in the **IP Address** field on the **General Properties** page.
Selected address from topology table	An IP address is selected from the list of IP addresses. These IP addresses are configured on the **Topology** page.
Statically NATed IP	A statically NATed IP address. The real IP address does not show in the topology table.

   - **Calculate IP based on network topology** - when a VPN peer tries to determine the IP address of the Security Gateway, the Security Gateway sends the list of its internal interfaces and the networks behind them to the client. The client checks if the IP address of one of its interfaces is on a network on this list. If a match exists, it establishes a connection with the matching IP address. Otherwise, it uses the IP address of the first external interface on the Security Gateway.

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

1. Save the changes.
2. Install Policy.

Machine Authentication

A Remote Access VPN client can use machine authentication to authenticate with a machine certificate.

Machine authentication supports these modes:

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

Machine authentication is supported for these Remote Access clients:

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

Machine authentication is not supported for Remote Access SecuRemote.

Machine Authentication Configuration on the Gateway

To configure Machine Authentication you must have a Security Gateway version that supports that feature. For the supported Security Gateway versions and the instructions for configuring Machine Authentication, see sk121173

Configuring the LDAP Server

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

To add and LDAP Server object as a trusted CA:

In the **Servers and OPSEC** tab, right-click **Servers** and select **Trusted CAs** > **New CA** > **Trusted**.

Configuring Machine Authentication on the Client

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

Available attributes:

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

  Default value: true.

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

  Default value: empty.

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

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

  Default value: true.

- `machine_tunnel_after_logon` - Lets the client ignore user authentication and authenticate using machine certificate only after a user logs in to the endpoint computer. If this attribute is set to true and the `machine_tunnel_site` has a value, and the value matches the display name of the created site, then authentication passes only with machine certificate after the user logs in to macOS.

  Default value: false.

To edit the attributes:

1. On the client computer, edit the `trac.defaults` configuration file in a plain-text editor, with Administrator permissions.
   - EPS (managed client):

     ```
     C:\Program Files (x86)\CheckPoint\Endpoint Security\Endpoint Connect\trac.defaults
     ```

   - EPC (standalone client):

     ```
     C:\Program Files (x86)\CheckPoint\Endpoint Connect\trac.defaults
     ```

2. Save the changes and close the editor.
3. Reboot the client computer.

Configuration Examples for Machine and User Authentication

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

Configuring machine and user authentication:

Establish a user and machine tunnel after a user logs in to the endpoint computer:

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

Configuring machine authentication before users log in to the endpoint computer, and user and machine authentication after users log in to the endpoint computer:

This procedure explains how to configure:

- Machine authentication before a user logs in to the endpoint computer.
- User and machine authentication after a user logs in to the endpoint computer.

A VPN tunnel is established automatically when the machine starts, and a machine certificate is used for authentication. After a user logs in to the endpoint computer, the VPN tunnel is disconnected. If **always connect** is enabled, a new VPN tunnel is established automatically using the user authentication method and machine certificate. This tunnel is established to the last site to which the user connected from the endpoint computer. When a user logs off from the endpoint computer, the VPN tunnel is disconnected, and a new VPN tunnel authenticated with a machine certificate is established.

1. Set `enable_machine_auth` to `true`.
2. Set `machine_tunnel_before_logon` to `true`.
3. Set `machine_tunnel_after_logon` to `false`.
4. Create the default site for the tunnel. (If this site is already defined, skip this step.)
5. Set the authentication method for the user (will be used after users log in to the endpoint computer).
6. Set `machine_tunnel_site` to the display name of the default site.

Configuring Machine tunnel authentication ('Terminal' mode):

A VPN tunnel is established automatically before the user logs in to the endpoint computer. The tunnel is maintained after the user logs in to the endpoint computer and after the user logs out of the endpoint computer.

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

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

Notes for machine tunnel authentication:

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

  To enable Always Connect:

  1. Open the VPN Client.
  2. Go to **VPN Options** > **Sites**
  3. Select a default site for machine only connection.
  4. Click **Properties** > **Settings**.
  5. Select **Enable Always Connect**.

Creating a Customized MSI file that Supports Machine Authentication

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

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

1. Install the Endpoint Client from the MSI you want to repackage.
2. Create a site, but do not connect to it. When asked for authentication method, keep the default value.
3. Edit the `trac.defaults` file and configure the machine tunnel.
4. To make sure that the client connects with a machine tunnel, restart the machine.

5. Copy the `trac.defaults` file and the `trac.config` file from the installation directory to a different directory.
6. Open the *"Creating Installation Package with VPN Configuration Utility" on page 36*:
   a. Choose the MSI you want to repackage.
   b. Select the **Replace trac.defaults file** and the **Replace trac.config file**.
   c. In the **Advanced** tab, select the VPN client sub type. To ask the user during the installation which flavor to install, leave it as **User defined (default).**

To upgrade from a Gateway with the customized MSI

See *"Upgrading with a Customized Package" on page 46*

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. In SmartConsole, open **Menu** > **Global Properties**.
2. Open **Remote Access** > **Endpoint Connect**.
3. Configure ***"Authentication Settings" on the next page***.
4. Configure **Connectivity Settings**:
   - ***"Connect Mode" on page 85***
   - ***"Location Aware Connectivity" on page 86***
   - ***"Roaming" on page 85***
   - ***"Idle VPN Tunnel" on page 88***
5. Configure **Security Settings**.
6. Configure ***"Configuring Upgrades" on page 46***.
7. Click **OK**.
8. Install policy.

Authentication Settings

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

To configure authentication settings:

- **Enable password caching**
  - **No** (default) - It requires users to enter a password whenever they connect.
  - **Yes** - It 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 is 480 minutes), after which users must re-authenticate the current connection.

  By default the re-authentication warning shows five minutes before the authentication timeout expires. To change the time, use the `reauth_grace_period` parameter in the file on the Security Gateway or in the `trac.defaults` (refer to *"The Configuration File" on page 138*):

  trac_client_1.ttm

```
:reauth_grace_period (
    :gateway (
        :default (10)
    )
)
```

  trac.defaults

```
reauth_grace_period   INT     10     GW_USER   0
```

  The Re-authentication warning window does not show:

  - Earlier that two minutes from the VPN session start

- Later than five minutes before the VPN session ends

If the administrator defines incorrect values, the default "five minutes" is used.

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

Connect Mode

In the **Connectivity Settings** of **Global Properties**> **Remote Access**> **Endpoint Connect**, configure how clients connect to the Security 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. This is also known as **always-connect** mode.
- **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. Close all SmartConsole windows.
2. Connect with Database Tool (GuiDBEdit Tool) to Security Management Server
3. In the upper left pane, go to the **Global Properties -global_properties**.
4. In the upper right pane, select **firewall_properties**.

5. Press **CTRL+F** (or go to the **Search** menu - **Find**) - paste **endpoint_vpn_implicit_disconnect_timeout** - click **Find Next**.
6. In the lower pane, right-click the **endpoint_vpn_implicit_disconnect_timeout** - select **Edit...** - enter the number of minutes that you want clients to roam before failing the connection - click **OK**.

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

1. Save the changes: go to the **File** menu - click **Save All**.
2. Close the Database Tool (GuiDBEdit Tool).
3. From the SmartConsole, install the policy on the Security Gateways.

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 Security Gateway interface that received the client connection. If the client connection came from an external interface of the Security Gateway, the client's location is considered to be in the external network. If the client connection came from an internal interface of the Security Gateway, the client's location is considered to be in the internal network. For an interface listed as both external and internal, the location is considered external.

- **Specific network considered as internal**

  The originating IP of the client connection, as seen from the Security Gateway, is compared to a configured list of internal networks. To use this setting, you must configure the internal networks.

- **Domain Controller (DC) connectivity** (default but limited)

  The location is based on the availability of the DC on the client network, assuming the DC is accessible only from within the internal network (not externally or through the VPN tunnel).

Enabling Location Awareness

To enable location awareness:

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

Configuring Location Awareness on Security Gateways

To configure Location Awareness on Security Gateways:

1. In SmartConsole, open **Global Properties** > **Remote Access** > **Endpoint Connect**.
2. In **Connectivity Settings**, in **Network Location Awareness**, select **Yes** and click **Configure**.

   The **Network Location Awareness** window opens.
3. Select a location awareness configuration.
   - **The client connects to the Security 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**.
5. Install policy.

Optimizing External Network Detection

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

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

- **Regard wireless networks as external** - Wireless networks you define here are internal. Of the client's wireless IP address is from one of these networks, it is considered internal. All other wireless networks are considered external.

- **Consider DNS suffixes which do not appear in the following list as external** - Define DNS suffixes that Remote Access Clients identifies as internal. If you select this option, make sure to define *all* internal DNS suffixes.
- **Remember previously detected external networks**. Networks previously identified by the client as external can be cached (on the client side), so future encounters with them result in immediate detection.

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

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

Idle VPN Tunnel

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

To configure tunnel idleness:

1. Close all SmartConsole windows.
2. Connect with Database Tool (GuiDBEdit Tool) to the Security Management Server.
3. In the upper left pane, go to the **Global Properties** > **global_properties**.
4. In the upper right pane, select **firewall_properties**.
5. Press **CTRL+F** (or go to the **Search** menu - **Find**) - paste **disconnect_on_idle** - click **Find Next**.
6. In the lower pane, and these parameters under **disconnect_on_idle**:
   - `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`
7. Save the changes: go to the **File** menu - click **Save All**.
8. Close the Database Tool (GuiDBEdit Tool).
9. From the SmartConsole, install the policy on the Security Gateways.

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 Security Gateway (for example, if there is a proxy or hotspot). Clients need Visitor Mode to operate.
- **NAT-T**- UDP encapsulation over port 4500 (by default) and preferable transport for IPSec. The IPSec protocol does not deal with NAT devices, so Remote Access Clients uses NAT-T encapsulation. NAT-T packets must go back to the client through the same interface they entered from. We recommend that you put the Security 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. Close all SmartConsole windows.
2. Connect with Database Tool (GuiDBEdit Tool) to the Security Management Server.
3. In the upper left pane, go to the the **Global Properties** > **global_properties**.
4. In the upper right pane, select **firewall_properties**.
5. Press **CTRL+F** (or go to the **Search** menu - **Find**) - paste **endpoint_vpn_ipsec_transport** - click **Find Next**.
6. In the lower pane, make sure the value of the **endpoint_vpn_ipsec_transport** parameter is **auto_detect**.
7. If made changes, save them: go to the **File** menu - click **Save All**.
8. Close the Database Tool (GuiDBEdit Tool).
9. From the SmartConsole, install the policy on the Security Gateways.

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. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Locate the `:disconnect_on_smartcard_removal` line:

   ```
   :disconnect_on_smartcard_removal (
    :gateway (
    :default (VALUE)
    )
   )
   ```

3. Change the **:default** value as required:
   - `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.
5. Install the policy.

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

Configuring Hotspot Access

Remote Access Clients users may need to access the VPN over the Internet from a public Wireless Hotspot or Hotel Internet portal.

The Desktop Policy may block hotspot access.

To let all your users connect to Hotspots as needed, configure these settings for SmartConsole-managed clients.

To enable hotspot registration:

1. In SmartConsole, open **Menu** > **Global Properties**.
2. Go to **Remote Access** > **Hot Spot/Hotel Registration**.
3. Select **Enable registration**.
4. Set the **Maximum** time and add **Ports** to be used.

5. Select a **Track** option.
6. Click **OK**.
7. Install the policy.

Note - **"Local subnet access only"** and **"Allow access to maximum of"** are not supported.

Configuring Automatic Hotspot Detection

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

Note - Hotspot detection requires outbound access to *vpnhotspot.checkpoint.com*
If this endpoint is blocked, hotspot detection and registration fail.

To enable hotspot registration from the configuration file:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Change these parameters:

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

Where:

Parameter	Default	Description
`hotspot_ detection_ enabled`	`true`	Enables (`true`) or disables (`false`) hotspot detection.

Parameter	Default	Description
`hotspot_registration_enabled`	`false`	Allows (`true`) or prevents (`false`) a user to get a hotspot registration page (in an embedded browser).

1. Save the file.
2. Install the policy on this Security Gateway.

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

Certificate Enhancements

On Remote Access VPN Windows Clients you can:

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

Configure these features in the `trac_client_1 ttm` configuration file.

To configure the new functionality:

In the `trac_client_1 ttm` configuration file, configure these parameters:

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

Warning When the Certificate is About to Expire

On Remote Access VPN Windows Clients you can show a notification to the user when a certificate is about to expire.

If you show this notification, the certificate is not renewed automatically.

If the user does not renew the certificate, then after the certificate expires the user will not be allowed to connect to protected resources.

The option to show the warning message is disabled by default.

To configure a warning to the user that the certificate is about to expire:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Set the value of the attribute `certificate_renewal_warning_only` to `true`.

   If the property does not exist, create it.
3. Save the file.
4. Install the policy on the Security Gateway.

Changes are applied the next time that the user connects.

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 private IP addresses (RFC 1918). It is best to encrypt the DNS resolution of these internal names.

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

You can configure multiple SecuRemote DNS servers for different domains.

Configuring Split DNS

To configure a SecuRemote DNS server for Split DNS:

1. Create a **New SecuRemote DNS**:

   - In SmartConsole, in the Objects tree, select **New** > **Server**> **More**> **SecuRemote DNS**.

   The **NewSecuRemote DNS** window opens.

2. In the **General** tab, enter a name for the server and select the host on which it runs.
3. In the **Domains** tab, click **Add** to add the domains that will be resolved by the server.

   The **Domain** window opens.

4. Enter the **Domain Suffix** for the domain that the SecuRemote DNS server will resolve, for example, checkpoint.com.
5. In the **Domain Match Case** section, select the maximum number of labels that can be in the URL before the suffix. URLs with more labels than the maximum will not be sent to that DNS.

   - **Match only *.suffix** - Only requests with 1 label are sent to the SecuRemote DNS. For example, "www.checkpoint.com" and "whatever.checkpoint.com" but not "www.internal.checkpoint.com."
   - **Match up to x labels preceding the suffix**- Select the maximum number of labels. For example, if you select 3, then the SecuRemote DNS Server will be used to resolve "www.checkpoint.com" and "www.internal.checkpoint.com" but not "www.internal.inside.checkpoint.com".

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

Enabling or Disabling Split DNS

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

To change the setting for Split DNS on the Security Gateway:

1. On the Security 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 required value in the `:default` attribute:
   - **true** - Enabled
   - **false** - Disabled (this is the default)
   - **client_decide** - Takes the value from a file on the client machine
4. Save the file.
5. Install the policy.

Configuring Log Uploads

You can have firewall and SCV logs from SmartConsole-managed clients sent to the Security Management Server.

Logs are accumulated by each client according to the Desktop Policy, and sent when the client next connects. You can see the logs in SmartConsole.

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. Edit the `$FWDIR/conf/trac_client_1.ttm` file on each Security Gateway.
3. Set the value of the `fw_log_upload_enable` parameter to `true`.

   If the value is `false`, the client does not accumulate logs, regardless of the rule's "Track" settings.
4. Save the file.
5. Install the policy.

Configuring Post Connect Scripts

The Post Connect feature runs a script or executable file on Remote Access VPN Client computers after they connect to the Security Gateway.

You must make sure that the script or executable file exists on the client computers, in the correct path.

Important Note - The Post-Connect script runs with user-level permissions. For security reasons, running the Post-Connect script is not supported if users do a Secure Domain Login before Windows login.

To configure the Post Connect script for all managed Remote Access Security Gateways:

1. Close all SmartConsole windows.
2. Connect with GuiDBEdit Tool to the Security Management Server / Domain Management Server.
3. In the upper left pane, go to the **Table** - **Global Properties** - **global_properties**.
4. In the upper right pane, select **firewall_properties**.
5. Press **CTRL+F** (or go to the **Search** menu - **Find**) - paste **desktop_post_connect_script** - click **Find Next**.
6. In the lower pane, make sure the attribute **desktop_post_connect_script** does not have any value (it is empty).

   If it has a value, then right-click this attribute and select **Reset**.
7. In the upper right pane, select **firewall_properties**.
8. Press **CTRL+F** (or go to the **Search** menu - **Find**) - paste **desktop_post_connect_script_show_window** - click **Find Next**.
9. In the lower pane, right-click the **desktop_post_connect_script_show_window** - select **Edit...** - select **"true"** - click **OK**.

   The default value is **false**. The script runs in a hidden window.
10. Save the changes: go to the **File** menu - click **Save All**.
11. Close the Database Tool (GuiDBEdit Tool).
12. Connect with SmartConsole to the Security Management Server / Domain Management Server.
13. Install the policy on each Security Gateway / Cluster object.

To configure the Post Connect script for a specific Remote Access Security Gateway:

1. Configure the path to the Post Connect script in the specific Security Gateway / Cluster:
   a. Close all SmartConsole windows.
   b. Connect with GuiDBEdit Tool to the Security Management Server / Domain Management Server.
   c. In the upper left pane, go to the **Table** - **Network Objects** - **network_objects**.
   d. In the upper right pane, select the relevant Security Gateway / Cluster object.
   e. Press **CTRL+F** (or go to the **Search** menu - **Find**) - paste **desktop_post_connect_script** - click **Find Next**.
   f. In the lower pane, make sure the attribute **desktop_post_connect_script** does not have any value (it is empty).

      If it has a value, then right-click this attribute and select **Reset**.
   g. In the upper right pane, select the applicable Security Gateway / Cluster object.
   h. Press **CTRL+F** (or go to the **Search** menu - **Find**) - paste **desktop_post_connect_script_show_window** - click **Find Next**.
   i. In the lower pane, right-click the **desktop_post_connect_script_show_window** - select **Edit...** - select **"true"** - click **OK**.
   j. The default value is **false**. The script runs in a hidden window.
   k. Save the changes: go to the **File** menu - click **Save All**.
   l. Close the Database Tool (GuiDBEdit Tool).
   m. Connect with SmartConsole to the Security Management Server / Domain Management Server.
   n. Install the policy on the specific Security Gateway / Cluster object.
2. Configure the Remote Access TTM file *$FWDIR/conf/trac_client_1.ttm* on the specific Security Gateway / each Cluster Member:

   Note - For more information about this TTM file, see sk75221.
   a. Connect to the command line on the Security Gateway / each Cluster Member.
   b. Log in to the Expert mode.
   c. Back up the current *$FWDIR/conf/trac_client_1.ttm* file:

      ```
      cp -v $FWDIR/conf/trac_client_1.ttm{,_BKP}
      ```

d. Edit the current *$FWDIR/conf/trac_client_1.ttm* file:

```
vi $FWDIR/conf/trac_client_1.ttm
```

e. Configure the path to the Post Connect script file:

Important - Such file must exist on all Remote Access VPN clients that connect to this Security Gateway.

```
:post_connect_script_show_window (
 :gateway (desktop_post_connect_script_show_window
 :valid (false)
 :default (true)
 )
)
:post_connect_script (
 :gateway (desktop_post_connect_script
 :valid (false)
 :default ("<Full Path to the script file on the Remote Access VPN computer>")
 )
)
```

For example:

```
:post_connect_script_show_window (
 :gateway (desktop_post_connect_script_show_window
 :valid (false)
 :default (true)
 )
)
:post_connect_script (
 :gateway (desktop_post_connect_script
 :valid (false)
 :default ("C:\vpn_pcs.bat")
 )
)
```

f. Save the changes in the TTM file an exit Vi editor.

g. From the SmartConsole, install the policy on the Security Gateway / Cluster object.

h. Delete the current VPN Site on the Remote Access VPN client.

i. Create the required VPN Site again on the Remote Access VPN client to download the new configuration from the Security Gateway / Cluster.

Configuring Post Disconnect Scripts

The *Post Disconnect Script* feature runs a script or executable file on the Remote Access VPN client computers after they disconnect from the Security Gateway.

You must make sure that the script or executable file exists on the client computers, in the correct path.

Important Note - The Post Disconnect script runs with user-level permissions. For security reasons, running the Post Disconnect Script is not supported if users do a Secure Domain Login before Windows login.

Do these steps on each applicable Security Gateway / each Cluster Member:

1. Connect to the command line on the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Back up the current `$FWDIR/conf/trac_client_1.ttm` file.
4. To configure the Post Disconnect feature, add these sections in the current `$FWDIR/conf/trac_client_1.ttm` file:

```
:post_disconnect_script_show_window (
    :gateway (
        :valid (false)
        :default (true)
    )
)

:post_disconnect_script (
    :gateway (
        :valid (false)
        :default ("<Full Path to the script file on the Remote
Access VPN computer>")
    )
)

:post_disconnect_mode (
    :gateway (desktop_post_disconnect_mode
```

```
        :valid (false)
        :default (1 or 2)
    )
)
```

5. Save the changes in the `TTM` file.
6. In SmartConsole, install the policy on the Security Gateway and, or Cluster Member.

New settings are effective on the next connection of the Remote Access VPN client computer to the Security Gateway and, or Cluster Member.

Notes:

- The "default" value of the "`post_disconnect_script_show_window`" is `true` or `false`.
  - To show the script window, set to `true`.
  - To hide the script window (this is the default), set it to `false`.
- The "default" value of the "`post_disconnect_script`" is the path to the script on the client's computer. The default value is an empty string.
- The "default" value of the "`post_disconnect_mode`" can be:
  - `0` - Feature is disabled (this is the default).
  - `1` - Only user-initiated events will run the script.
  - `2` - All events will run the script
- For example, “Should you need to turn off the Post Disconnect Script. To turn it off you should set “`0`” to the value of the "`post_disconnect_mode`".

In addition, you can configure the Post Disconnect Script through the `trac.defaults` file.

To enable Post Disconnect Script:

1. Go to the **Endpoint Connect** program folder:
   - 64-bit systems - `%programfiles(x86)%\CheckPoint\Endpoint Connect\`
   - 32-bit systems - `%programfiles%\CheckPoint\Endpoint Connect\`
2. Edit the `trac.defaults` file in a plain-text editor, such as Notepad.
3. Set applicable values for these parameters:

post_disconnect_script STRING "<Full Path to the script file on the Remote Access VPN computer>" GW_USER 0

```
post_disconnect_script STRING "<Full Path to the script file on
the Remote Access VPN computer>" GW_USER 0
post_disconnect_
script                          STRING        "<Full Path to the
script file on the Remote Access VPN computer>"      GW_
USER     0

post_disconnect_script_show_
window              STRING        <true or
false>                   GW_USER     0

post_disconnect_mode                              INT           <1
or 2>                       GW_USER     0
```

4. Save the file.
5. Open the Command Prompt as Administrator and run:

   ```
   > net stop TracSrvWrapper
   ```

   ```
   > net start TracSrvWrapper
   ```

To disable Post Disconnect Script:

1. Go to the **Endpoint Connect** program folder:
   - 64-bit systems - `%programfiles(x86)%\CheckPoint\Endpoint Connect\`
   - 32-bit systems - `%programfiles%\CheckPoint\Endpoint Connect\`
2. Edit the `trac.defaults` file in a plain-text editor, such as Notepad.
3. Find the `post_disconnect_mode` parameter and set its value to "`0`".
4. Save the file.
5. Open the Command Prompt as Administrator and run:

   ```
   > net stop TracSrvWrapper
   ```

   ```
   > net start TracSrvWrapper
   ```

Office Mode IP Address Lease Duration

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

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

When using a DHCP server to assign IP addresses to users, the DHCP server's configuration determines the IP lease duration. When a user disconnects and reconnects to the Security Gateway within a short period of time, it is likely that the user will get the same IP address as before.

No Office Mode - Secondary Tunnel Resilience

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

New features:

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

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

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

Secondary Tunnel Resilience

Terminology:

- **Primary Gateway**

  The Security Gateway responsible for client configuration.

- **Secondary Gateway**

  The second Security Gateway in a tunnel.

- **Default Gateway**

  The Security Gateway chosen as first to connect.

- **Roaming**

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

How Secondary Tunnel Resilience Works

Connection State	If Tunnel is Disconnected From:	Roaming Tries to:
Tunnel to Primary Gateway (A) is connected	Primary Gateway (A)	Reconnect the tunnel.
Primary Gateway (A) and Secondary Gateway (B) are connected	Primary Gateway (A)	Reconnect the tunnel to the Primary Gateway (A). If roaming timeout is reached, the tunnel to the Primary Gateway (A) is disconnected. The Secondary Gateway (B) stays connected and is defined as the Primary Gateway. The tunnel to Gateway (A) is connected again with the encryption domain resource access, as Secondary Tunnel.
Primary Gateway and Secondary Gateway are connected	Secondary Gateway (B)	Reconnect the tunnel. Nothing changes in the client state.

Match the VPN User to the Logged-In Windows User

Starting from E81.20, added the ability to match the VPN user to the logged-in Windows user and display it in the username field of the connect dialog for the username-password authentication method.

On the first attempt to connect to the Security Gateway, the username field is empty. In subsequent attempts, the username field shows the last connected VPN username for the currently logged-in Windows user.

The number of saved VPN usernames on each machine is 10 by default. This value is configurable and can be set to unlimited.

Configuration

This feature is disabled by default with the following attributes:

- *save_vpn_user_per_sid* - The valid values are *true* and *false* to enable and disable the feature.
- *max_num_of_users_to_save* - The default is set to *10*. The valid values are positive integers to limit the number of users to save on each client machine.

To enable this feature:

1. Edit the `$FWDIR/conf/trac_client_1.ttm` file on the Security Gateway.
2. Add these lines:

```
:save_vpn_user_per_sid (
 :gateway (
 :default (true)
 )
)
```

3. Save the file.
4. Install policy.
5. Apply this configuration to all Security Gateways.

Remote Access Clients 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 the Windows command prompt.

   Note - If you are using Windows 7 (or above) User Account Control (UAC), open the Command Prompts as Administrator.

2. Browse to the Remote Access clientsdirectory:

   - 32-bit system:

     `C:\Program Files\CheckPoint\Endpoint Connect\trac`

   - 64-bit system:

     `C:\Program Files (x86)\CheckPoint\Endpoint Connect\trac`

3. Run:

   `trac <command> <arg>`

CLI Commands

These commands can be used for Remote Access Clients.

change_p12_pwd

Section/Topic	Description
Description	Changes the password of a p12 certificate.
Syntax	`trac change_p12_pwd -f <filename> [-o <old password> -n <new password>]`

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Arguments</td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<tr><td>-s</td><td>name of the site</td></tr>
<tr><td>-f</td><td>pathname to the certificate file</td></tr>
<tr><td>-o</td><td>old password for the certificate</td></tr>
<tr><td>-n</td><td>new password for the certificate</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td>

```
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:****
```

</td></tr>
</table>

connect

Section/Topic	Description
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>]`

Section/Topic	Description
Arguments	<table><tr><th>Args</th><th>Description</th></tr><tr><td>-s</td><td>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.</td></tr><tr><td>-g</td><td>Name of the Security 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.</td></tr><tr><td>-u and -p</td><td>username and password credentials</td></tr><tr><td>-d</td><td>DN</td></tr><tr><td>-f -p</td><td>pathname and password of P12 certificate file</td></tr><tr><td>-pin and -sn</td><td>SecurID PIN and passcode</td></tr></table>

connectgui

Section/Topic	Description
Description	Connects to the Security Gateway using the GUI. The GUI must be running. If a user's authentication credentials are not cached, it opens the login page so the user can authenticate. If the name of the site is not entered, the client connects to the active site.
Syntax	`trac connectgui [-s <site name>]`
Arguments	`[-s <site name>]` – name of the site to connect to

create

Section/Topic	Description
Description	Creates a new site and defines its authentication method. Example: `"C:\Program Files (x86)\CheckPoint\Endpoint Connect\trac.exe" create`
Syntax	`trac create -s <site> [-di <display name>] [-a <auth method>] [-lo <login option>] [-f <fingerprint>]`

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Arguments</td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<tr><td><code>-s</code>
(Mandatory)</td><td>The site's name (FQDN or IP Address).

You can use the gateway's Fully Qualified Domain Name or its IP address. This is the site's name, unless configured with <code>-di</code>.

Examples:
<code>"C:\Program Files (x86)\CheckPoint\Endpoint Connect>trac.exe" create -s 192.168.1.1</code>
<code>"C:\Program Files (x86)\CheckPoint\Endpoint Connect>trac.exe" create -s example.com</code></td></tr>
<tr><td><code>-di</code>
(Optional)</td><td>The site's display name.

This is used to change the display name of the site after its creation. By default, it takes the value of <code>-s</code>. The name must be in double quotes if the display name requires a space.

Examples:
<code>"C:\Program Files (x86)\CheckPoint\Endpoint Connect>trac.exe" create -s 192.168.1.1 -di "Main Gateway"</code>
<code>"C:\Program Files (x86)\CheckPoint\Endpoint Connect>trac.exe" create -s 192.168.1.1 -di "Main Gateway" -lo "Username Password"</code></td></tr>
</table>
</td></tr>
</table>

Section/Topic	Description

Args	Description
`-a` (Optional)	If there are multiple possible authentication methods for the selected login option, for example, `CAPI certificate vs. p12 certificate`, then you can specify which method the site must use. A list of valid values: ■ `username-password` ■ `certificate` (for a CAPI certificate) ■ `p12-certificate` ■ `challenge-response` ■ `securIDKeyFob` ■ `securIDPinPad` ■ `SoftID`
`-lo` (Optional)	Used to select the login option for the site. It is necessary to enter the display name as it is configured in SmartConsole in the **Gateway Settings** > **VPN Clients** > **Authentication**. If there is a space in the Authentication Method's display name, then it must be in double quotes. This argument is not necessary if there is only one login option configured on this gateway. It is not possible to connect from the command line to a Security Gateway with a login option that has more than one authentication factor configured. If it was configured as such, then this error shows: `unsupported notification id` Example: `"C:\Program Files (x86)\CheckPoint\Endpoint Connect>trac.exe" create -s 192.168.1.1 -lo Standard -a username-password`

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<tr><td colspan="2">Note - If <code>-lo</code> and <code>-a</code> are not configured, the command line might request to know the login option or authentication method for the site (if there is more than one option).
If it is necessary to have the command line site creation continue without user input, then you must configure each of the arguments in the command.</td></tr>
<tr><td>-f
(Optional)</td><td>The expected site’s fingerprint.
<code>-f</code> is useful to skip a request for a Root CA fingerprint approval for newly created sites. <code>-f</code> is ignored if the Root CA fingerprint is already stored on the computer.</td></tr>
</table>
</td></tr>
<tr><td>Examples</td><td>

<code>trac create -s mygateway.example.com -a certificate -lo Standard</code>
<code>trac create -s mygateway.example.com -di "My Gateway" -a certificate -lo Standard -f "LEFT SAN MEND SLAT MUTE STAB GURU BOLT FRET SAT CORE LA"</code>

</td></tr>
</table>

delete

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Description</td><td>Deletes a site definition.</td></tr>
<tr><td>Syntax</td><td><code>trac delete -s <site></code></td></tr>
<tr><td>Arguments</td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<tr><td><code>-s</code></td><td>name of the site</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td><code>trac delete -s mygateway.domain.com</code></td></tr>
</table>

disable_log

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Description</td><td>Stops logging.</td></tr>
</table>

Section/Topic	Description
Syntax	`trac disable_log`
Arguments	none

disconnect

Section/Topic	Description
Description	Disconnects the local client from the current connection.
Syntax	`trac disconnect [-g <gateway>]`
Arguments	**Args** / **Description** -g / Name of gateway to disconnect. Optional parameter that can be used to disconnect a specified tunnel. If not given, the client disconnects the active site.

enable_log

Section/Topic	Description
Description	Enables logging.
Syntax	`trac enable_log [-m <logging mode>]` **Note** - The "`-m <logging mode>`" option is available starting from E82.10.
Arguments	**Args** / **Description** `-m` / Logging mode. Valid values.: ■ Basic ■ Extended No arguments is equivalent to `-m basic`.

enroll_capi

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Description</td><td>Enrolls a CAPI certificate.</td></tr>
<tr><td>Syntax</td><td><pre>trac enroll_capi -s <site> -r <key> [-i <providerindex> -l <keylength> -sp <strongkeyprotection>]</pre></td></tr>
<tr><td>Arguments</td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<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
(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
(Valid values: "true" or "false")</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td><pre>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</pre></td></tr>
</table>

enroll_p12

Section/Topic	Description
Description	Enrolls a p12 certificate.
Syntax	`trac enroll_p12 -s <site> -f <filename> -p <password> -r <key> [-l <keylength>]`

Section/Topic	Description
Arguments	<table><tr><th>Args</th><th>Description</th></tr><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></table>
Example	`trac enroll_p12 -s mygateway.domain.com -f "d:\My Documents\certs\mycert.p12" -p mypass -r 654321`

firewall

Section/Topic	Description
Description	Enables or disables the Desktop firewall
Syntax	`firewall -st enable|disable`
Arguments	None

get_cross_gws_intersections

Section/Topic	Description
Description	Shows intersections of IP address ranges between gateways in a given site.
Syntax	`firewall -st enable|disable`
Arguments	<table><tr><th>Args</th><th>Description</th></tr><tr><td>-s</td><td>The name of the site</td></tr></table>
Example	`trac get_cross_gws_intersections -s MyOrg-Site-1`

get_cross_site_intersections

Section/Topic	Description
Description	Shows intersections of IP address ranges between all configured sites.
Syntax	`trac get_cross_site_intersections`
Arguments	None
Example	`trac get_cross_site_intersections`

help

Section/Topic	Description
Description	Outputs help on the CLI or for a command.
Syntax	`trac help | h`
Arguments	none, but if a command is given, help for that command is shown

hotspot_reg

Section/Topic	Description
Description	Temporarily allows endpoint connections from Hotspots in public places, such as airports and hotels, so that the user can register with the Hotspot portal.
Syntax	`hotspot_reg`
Arguments	none

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

info

Section/Topic	Description
Description	Outputs all sites configured and their gateways, including current tunnel status.
Syntax	`trac info [-s <site name>]`

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Arguments</td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<tr><td><code>-s</code></td><td>name of the site
If given, only gateways and tunnel information for this site are shown.</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td><pre>trac info
trac info -s mygateway.domain.com</pre></td></tr>
</table>

List

Section/Topic	Description
Description	Shows certificate subject names stored in the CAPI.
Syntax	`trac List`
Arguments	none

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

Log

Section/Topic	Description
Description	Shows messages for "no network" and "service is down".
Syntax	`trac Log`
Arguments	none

Section/Topic	Description

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

Section/Topic	Description
Description	Renews a capi certificate.
Syntax	`trac renew_capi -s <sitename> -d <dn> [ -l <keylength> -sp <strongkeyprotection> ]`
Arguments	<table><tr><th>Args</th><th>Description</th></tr><tr><td>-s</td><td>name of the site</td></tr><tr><td>-d</td><td>certificate subject name</td></tr><tr><td>-l</td><td>length of the registration key</td></tr><tr><td>-sp</td><td>if strong key protection is used (Valid values: "true" or "false")</td></tr></table>
Example	`trac renew_capi -s 192.0.2.0 -d CN=yCert,OU=users,O=cpmodule..p86dj5`

renew_p12

Section/Topic	Description
Description	Renews a p12 certificate.
Syntax	`trac renew_p12 -s <site> -f <filename> -p <password> [-l <keylength>]`

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Arguments</td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<tr><td><code>-s</code></td><td>name of the site</td></tr>
<tr><td><code>-f</code></td><td>pathname for the certificate file</td></tr>
<tr><td><code>-p</code></td><td>password for the certificate</td></tr>
<tr><td><code>-l</code></td><td>length of the key</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td><code>trac renew_p12 -s mygateway.domain.com -f "<full path> mycert.p12" -p mypass</code></td></tr>
</table>

set_proxy_settings

<table>
<tr><th>Section/Topic</th><th>Description</th></tr>
<tr><td>Description</td><td><code>trac set_proxy_settings [-m <mode>] [-h <hostname> -po <port>] [-u <username> -p <password>]</code></td></tr>
<tr><td>Arguments</td><td>
<table>
<tr><th>Args</th><th>Description</th></tr>
<tr><td><code>-m mode</code></td><td>one of no_proxy | manual | auto no_proxy - To disable proxy setting auto - To take proxy settings from the Internet Explorer LAN Settings manual - To set the proxy address (i.e. hostname and port)</td></tr>
<tr><td><code>-h</code>
<code>-p</code></td><td>hostname and port of the proxy
This can be set only when the proxy mode is manual</td></tr>
<tr><td><code>-u</code>
<code>-p</code></td><td>username and password credentials
This can be set only when the proxy mode is not no_proxy</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td><code>trac set_proxy_settings -m manual -h 192.168.1.1 -po 12345 -u user -p pass</code></td></tr>
</table>

start

Section/Topic	Description
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

Section/Topic	Description
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

Section/Topic	Description
Description	Shows the version of the client.
Syntax	`trac Ver`
Arguments	none

sdl

Section/Topic	Description
Description	Enable or disable Secure Domain Logon (SDL).
Syntax	`trac sdl -st <state>`

Section/Topic	Description
Arguments	<table><tr><th>Args</th><th>Description</th></tr><tr><td>-st</td><td>SDL state - "enable" / "disable"</td></tr></table>
Example	`trac sdl -st enable` `trac sdl -st disable`

userpass

Section/Topic	Description
Description	For ATM clients, sets the username and password.
Syntax	`trac userpass -s <sitename> -u <username> -p <password>`

Example	To set username and password:
	`trac userpass -s <sitename> -u <username> -p <password>`
	To delete username and password:
	`userpass -s <sitename>`

certpass

Section/Topic	Description
Description	For ATM clients, sets the certificate path and password.
Syntax	`trac certpass -s <sitename> -f <certificate filename> -p <password>`

Example	To set username and password:
	`trac certpass -s <sitename> -f <certificate filename> -p <password>`
	To delete certificate credentials:
	`certpass -s <sitename>`

Monitoring and Troubleshooting

This section describes different options of Remote Access clients monitoring and troubleshooting.

Collecting Logs

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

For SmartConsole-managed clients, users can send log files with their default email account. You can configure the client for your email address.

To define a default email address for log files:

1. Edit the **$FWDIR/conf/trac_client_1.ttm** file on the Security Gateway.
2. Enter a default email address (enclosed in double quotes) in the default value of the `send_client_logs` attribute:

   ```
   :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.
4. Install the policy.

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

You will get the email after the user click **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 here:
  `%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.

Filename	Description	Notes
AdminMode.bat	Opens the client with the Administrator tab, to generate a new MSI package.	
DLLs		Some DLLs install SCV checks on client computers.
trac.log*	Logs of the client service actions.	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.
cpmsi_tool.exe	CLI for updating an MSI.	This is the same tool that is launched from the Administrator tab, when the client is in AdminMode.
trac.exe	*"Remote Access Clients Command Line" on page 106*.	

Filename	Description	Notes
TracSrvWrapper.exe	The Remote Access Clients service.	
update_config_tool.exe	CLI of the update tool.	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.
TRAC.cab	The client MSI and other installation files on the Security Gateway.	In most cases, this file is not on client computers.
desktop_policy.ini	The desktop policy.	
user_group.ini	Groups that the authenticated user belongs to.	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.
vna.sys	driver	
cpgina.log, cpplap.log	Logs for Remote Access Clients support for Windows SDL by GINA and PLAP.	
helpdesk.log	Log of basic actions of the client service.	Logged events include: connect, disconnect, idle, upgrade, and similar client actions.
trac_fwpktlog.log	Log of firewall activity with rule number.	Display firewall packet drop and accept logs.

Filename	Description	Notes
collect.bat	Collects logs.	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.
LangPack1.xml	Translated resource files.	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.

Error Messages

Unsupported Services

Symptom	Client shows an error message: `Firewall policy contains unsupported services. Contact your system administrator`
Causes	Clients do not recognize all services that are in policy rules.
Solution	1. Open the `trac.log` file. 2. Find: `ConvertRule: ERROR - BuildProtocolString failed!!` 3. Go up two lines and find the rule number: `ConvertRule: rule = rule-`<number>`, start converting...` 4. Open the `desktop_policy.ini` file 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 SmartConsole. 7. Find the rule in the **Desktop** policy. 8. Remove the unsupported service from the rule. 9. Install the Desktop policy.

Login option not configured

Symptom	Client shows an error message: `Connection failed. Login option not configured.`
Causes	A login option was changed on the Security Gateway and the user must select a new login option.
Solution	Users click the link **Click here to configure Login Option**. This takes them to the **Authentication** tab of the client, where they can select a different login option.

Configuring No-Router Environments

You must configure the server in SmartConsole if there is no router between the Security 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 SmartConsole, open the properties of the Remote Access Clients Security Gateway.
2. Open **IPSEC VPN** > **Office Mode**:
3. Select the **Multiple Interfaces** option **Support connectivity enhancement for gateways with multiple external interfaces**.
4. Click **OK**.
5. Install policy.

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. Open the Security Gateway Properties window of the Remote Access Clients gateway.
2. Open **IPSec VPN** > **Office Mode.**
3. Click **Offer Office Mode to group** or **Allow Office Mode to all users**.
4. Click **Optional Parameters**.
5. Increase the value of **IP lease duration**.

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

Troubleshooting the Firewall

To troubleshoot the firewall, you can use these tools:

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

Using the Windows Service Query

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

Service Name	vsdatant
Description	Check Point service for the desktop policy firewall.
Syntax	`sc query vsdatant`
Example Output	`STATE : 4 Running` `<STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN>`

Desktop Firewall Monitoring

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

PacketMon:

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

VSDATANT:

- Initializes input and output buffers.
- Runs each incoming and outgoing packet through the INSPECT virtual machine.

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

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

If an error occurs, this usage message shows:

```
packetmon [-h] [-t] [-T] [-i] <{-e expr}+|-f <filter_file|->> [-l
len] [-
m mask] [-x offset[,len]] [-o file] [-ci count] [-co count] -I -d
-r
 -e expr: filters packets according to the given expr regular
expression
 -l len: limits packet capture length to the given len bytes
 -m mask: captures packets according to the given mask
 mask can be combination of:
 i - incoming packets (while entering the firewall)
 I - incoming packets (while leaving the firewall)
 o - outgoing packets (while entering the firewall)
 O - outgoing packets (while leaving the firewall)
 -x offset[,len]: prints packet data starting from the given
offset and
 for an optional number of bytes (len). offset is the offset from
the
 beginning of the IP header
 len can be used to limit the amount of bytes printed. If omitted
will
 print the whole packet from the given offset to its end
 -o file: write output to the given file (in snoop file format)
 -ci count: captures count number of incoming packets and exits
 -co count: captures count number of outgoing packets and exits
 -I: shows interface numbers instead of names
 -f filter_file: filters packets according to the regular
expression given
 in the filter_file file
 -f -: filters packets according to the regular expression given
in the
 standard input
 Ctrl-Z+<Enter> at a new line to stop stdin input
 -d: shows only dropped packets
 -r: prints relevant rule (if found)
 -T: prints time stamp
 -h: shows this help message
 -i: flushes standard output
 -t: do not include fwmonitor.def file automatically
```

Running PacketMon

1. Open a command prompt.
2. Change directory to the Remote Access Clients installation folder.
3. Run: `packetmon`.

Note -
- You can only run one instance of `PacketMon.exe` at a time.
- To stop packet monitoring, press `Ctrl-c`.

Command Syntax in Detail

-h

Purpose	Shows command usage
Example	`packetmon -h`

-e expr

Purpose	Filters packets according to the given INSPECT expression (expr)
Example	`packetmon -e "tcpport(23), accept;"`
Default	If the -e option is not given, all packets are captured. This option is the same as running: `packetmon -e "accept;"` **Note**: The -e option cannot be used with the -f option. See also the `-t` option.

-f file

Purpose	This option filters packets according to INSPECT expressions in a given file. To use pre-defined INSPECT macros, the given file must include the '`#include "fwmonitor.def"`' directive. **Note**: The -f option cannot be used with the -e option.
Example	`packetmon -f inspect.dat`

	Inspect.dat contents:
	`#include "fwmonitor.def"`
	`tcpport(23), accept;`

-f

Purpose	This option filters packets according to INSPECT expressions given in the standard input. To use pre-defined INSPECT macros, the input must include the directive: `#include "fwmonitor.def"` To stop command input and start packet inspection based on the given input, enter `Ctrl-Z+<Enter>` at a new line. **Note**: The `-f` option can not be used with the `-e` option.

Example	`packetmon -f -`
	
	Standard input contents:
	`#include "fwmonitor.def"`
	`tcpport(23), accept;`
	`Ctrl-Z+<Enter>`

-t

Purpose	The `fwmonitor.def` file includes all the INSPECT predefined macros you can use with the -e option. \The `Fwmonitor.def` file is included automatically when you use the `-e` option. If you want to define new macros with the same name as those defined in `fwmonitor.def`, use the `-t` option to exclude `fwmonitor.def`, and include your own definition file.

-l len

Purpose	Limits packet capture length to the given `len` bytes. Note: len indicates number of bytes to capture starting at the IP header. Regardless of the `len` value, the MAC header is always captured.
Example	`packetmon -l 20`
Default	If the -l option is not given, all packet data is captured
Comment	■ This option is useful if you have to debug highly sensitive communication data. The options lets you capture only the headers of a packet (e.g. IP and TCP header) while omitting the actual sensitive payload. You can debug the communication without seeing the actual data transmitted. ■ On computers experiencing a heavy load, you can use this option to reduce the file size by omitting the payload. The packetmon utility uses a buffer to transfer the packets from Kernel to user space. Reducing the packet length slows the rate at which the buffer fills.

-m mask

Purpose	By default packetmon captures packets before and after firewall inspection. The `-m` option lets you to specify capture on: ■ `i` Inbound packets before firewall inspection. ■ `I` Inbound packets after firewall inspection. ■ `o` Outbound packets before firewall inspection ■ `O` Outbound packets after firewall inspection The mask can be a combination of the above.
Example	`packetmon -m IO`
Default	Not specifying the `-m` option is the same as running: `packetmon -m iIoO`

-x offset [, len]

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

-o file

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

-ci count / -co count

Purpose	This option limit the number of packets being captured. This is useful when you need to troubleshoot a firewall handling large amounts of traffic. ■ `-ci` Defines how many inbound packets to capture ■ `-co` Defines how many outbound packets to capture
Examples	`packetmon -ci 5` `packetmon -ci 3 -co 10`

-I

Purpose	To avoid long interface names, this option prints the index of the interface on which the packet was received or sent. After the packet capture is stopped, a list of all interfaces (index and names) is printed.
Example	`packetmon -I`
Default	If the option is not specified, the interface name is printed.

-d

Purpose	This option shows packets dropped by the firewall. Use this option when you need to locate a packet missing from the output.
Example	`packetmon -d`
Default	Without this option, packetmon shows packets before they pass through the FW engine (i/o) and packets accepted by the FW engine (I/O). Packet that are dropped are not shown.

-r

Purpose	If a packet is dropped or accepted because of a rule, this option prints the name and the ID of the rule.
Example	`packetmon -r`

-T

Purpose	This option prints the time stamp for each packet.
Example	packetmon - T

-i

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

Major INSPECT macros supported by PacketMon

IP Header

Macro	Purpose	Example
ip_tos	Type Of Service field	ip_tos=1
ip_len	Total Length field	Ip_len=20
ip_id	Identification field	ip_id=100
ip_off	Flags and Fragment Offset fields	ip_off>0
ip_ttl	TTL field	ip_ttl<80
ip_p	Protocol field	ip_p=6
ip_sum	Header Checksum field	ip_sum!=0
src	Source address field	src=194.29.35.43
dst	Destination address field	dst=194.29.35.43

TCP

Macro	Purpose	Example
sport	Source port	sport=21
dport	Destination port	dport=21
th_seq	Sequence Number	th_seq=0
th_ack	Acknowledgment Number	th_ack>0
th_flags	Control Bits	th_flags=TH_RST
th_win	Window	th_win>128
th_sum	Checksum	th_sum!=0

Macro	Purpose	Example
th_urp	Urgent Pointer	th_urp!=0
syn	SYN flag is set	syn
fin	FIN flag is set	fin
rst	RST flag is set	rst
ack	ACK flag is set	ack
first	First TCP packet (only SYN is set)	first
established	TCP handshake completed	established
not_first	Not first packet (SYN flag is not set)	not_first
last	Last TCP packet	last
tcpdone	FIN or RST flags are set	tcpdone

UDP

Macro	Purpose	Example
sport	Source port	sport=21
dport	Destination port	dport=21
uh_ulen	length	uh_ulen>100
uh_sum	Checksum	uh_sum=0

ICMP

Macro	Purpose	Example
icmp_type	Type	icmp_type=ICMP_ECHOREPLY
icmp_code	Code	icmp_code=ICMP_UNREACH_NET
icmp_cksum	Checksum	icmp_cksum=0

Useful INSPECT macros supported by PacketMon

Accept Specified Protocol Only

Macro	Purpose	Example
tcp	Accept only TPC protocol	tcp
udp	Accept only UDP protocol	udp
icmp	Accept only ICMP protocol	icmp

Accept packets to or from a host or port

Macro	Purpose	Example
host	Accept only from given source or destination IP address	host (91.90.128.4)
tcpport	Accept only TCP packets with given source or destination port number	tcpport(21)
udpport	Accept only UDP packets with given source or destination port number	udpport(500)
port	Accept only TCP or UDP packets with given source or destination port number	port(300)

Accept packets to or from computers on a specified network

Macro	Purpose	Example
from_net	Accept only packets coming from the given network (source IP)	from_net (91.90.0.0,16)
to_net	Accept only packets sent to the given network (destination IP)	to_net (91.90.128.0,24)
net	Accept only packets coming from or going to the given network	net(194.29.35.0,24)

Accept specified ICMP types

Macro	Purpose	Example
icmp_error	Accept ICMP errors	icmp_error
echo_req	Accept only ICMP echo requests	echo_req
echo_reply	Accept only ICMP echo replies	echo_reply
ping	Accept only ICMP echo requests and replies	ping

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.

The Configuration File

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

Editing the TTM File

When the client connects to the Security Gateway, the updated policy is downloaded to the client and written in the `$FWDIR/conf/trac.config` file.

If you make changes in the `$FWDIR/conf/trac_client_1.ttm` file of a Security Gateway, you must install the policy on the Security Gateway.

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

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

To activate changes in the TTM file:

1. Edit and save the file.
2. Install the policy in one of these ways:
   - In SmartConsole, select **Install Policy** and install Access Control on each changed Security Gateway.
   - Run `cpstop` and `cpstart` from the CLI of each changed Security 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 Security Gateway is identical, you can manage one copy of the configuration file on the Security Management Server. This file is copied to the Security Gateways when you install the policy.

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

To centrally manage the configuration file on gateways:

1. On the Security Gateway, save a backup of the `$FWDIR/conf/trac_client_1.ttm` file.

   For CMA specific:

   a. On the MDS, run `mdsenv CMA_NAME`.

   b. Copy the `$FWDIR/conf/trac_client_1.ttm` file from the Security Gateway to the MDS's `$FWDIR/conf/ directory` in the CMA.

   c. Edit the `$FWDIR/conf/fwrl.conf` file on the Security Management Server in the CMA.

   For all MDS:

   a. Copy the `$FWDIR/conf/trac_client_1.ttm` file from the Security Gateway to the MDS's `$MDS_FWDIR/conf/ directory`.

   b. Edit the `$MDS_FWDIR/conf/fwrl.conf` file on the Security Management Server.

2. Find this section: `% SEGMENT FILTERLOAD`

3. In the `NAME` section, add this line:

   ```
   NAME = conf/trac_client_1.ttm; DST = conf/trac_client_1.ttm;
   ```

   This copies the `trac_client_1.ttm` file to the Remote Access clients Security Gateways each time you install the policy on them.

4. Save the file.

5. From the SmartConsole, install the policy on all gateways (policy acceleration must be canceled).

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

Understanding the Configuration File

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

```
: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 Security 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 Security 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 Security Gateway. Do not change it. This function can be done in addition to the function defined for the attribute on the client or Security Gateway side.
- **map** - Contains the valid values this attribute can have.
- **default** - The value here is downloaded to the client if the Security 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 Security Gateway in `objects.c` file on the Security Management Server, that value is used.
2. If the **attribute** is NOT defined for a Security 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:

```
:enable_password_caching (
        : ()
                :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 Security Gateway.

- If the attribute is defined for the Security 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

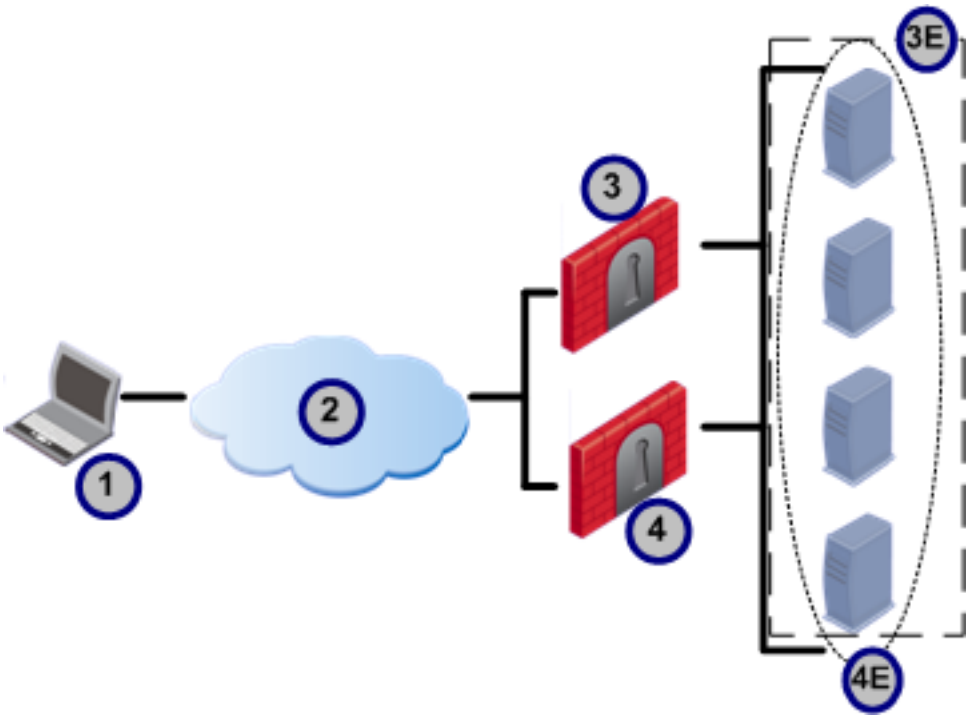
See sk75221 for an updated list of parameters for the configuration file.

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 Security Gateway. This is based on the topology configured for the Security Gateway. Alternatively, you can set a different domain for the Remote Access Community from the **Topology** page of the Security 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.



Item	Description
1	Remote Access Client
2	Internet
3	Gateway A
3E	Encryption Domain for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B

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.

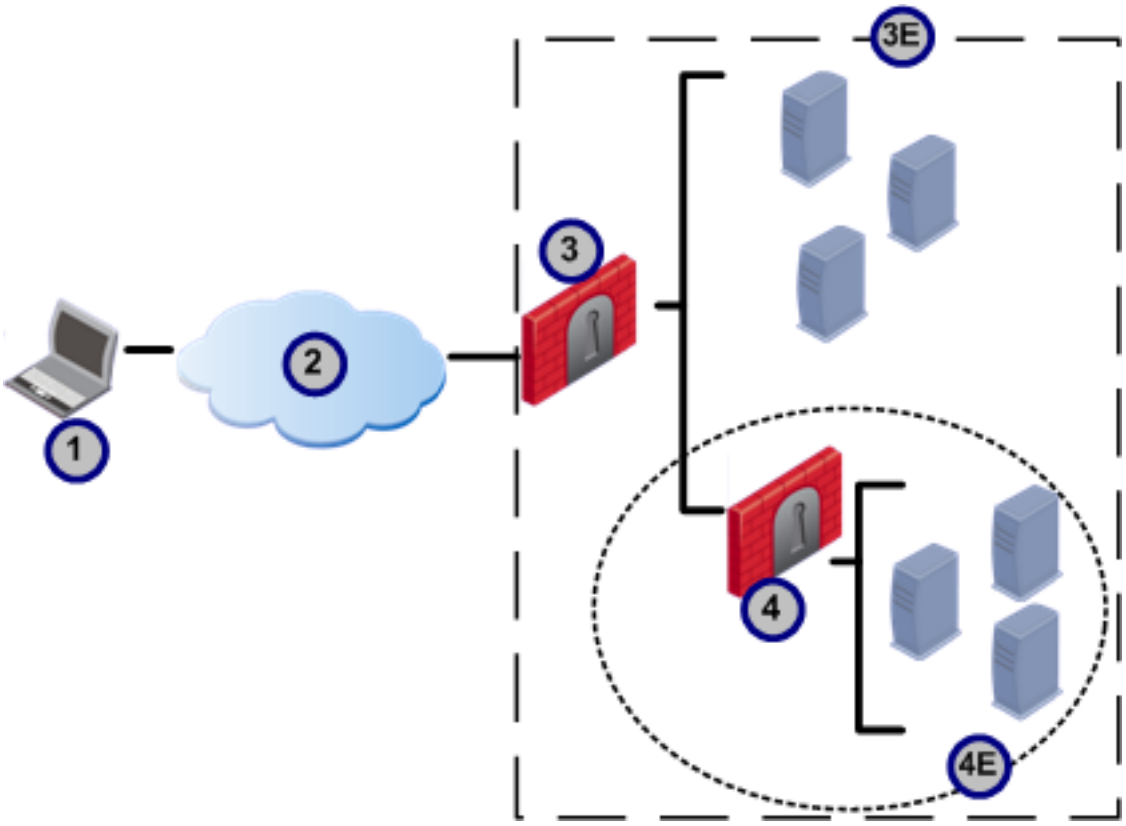
Proper Subset

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.

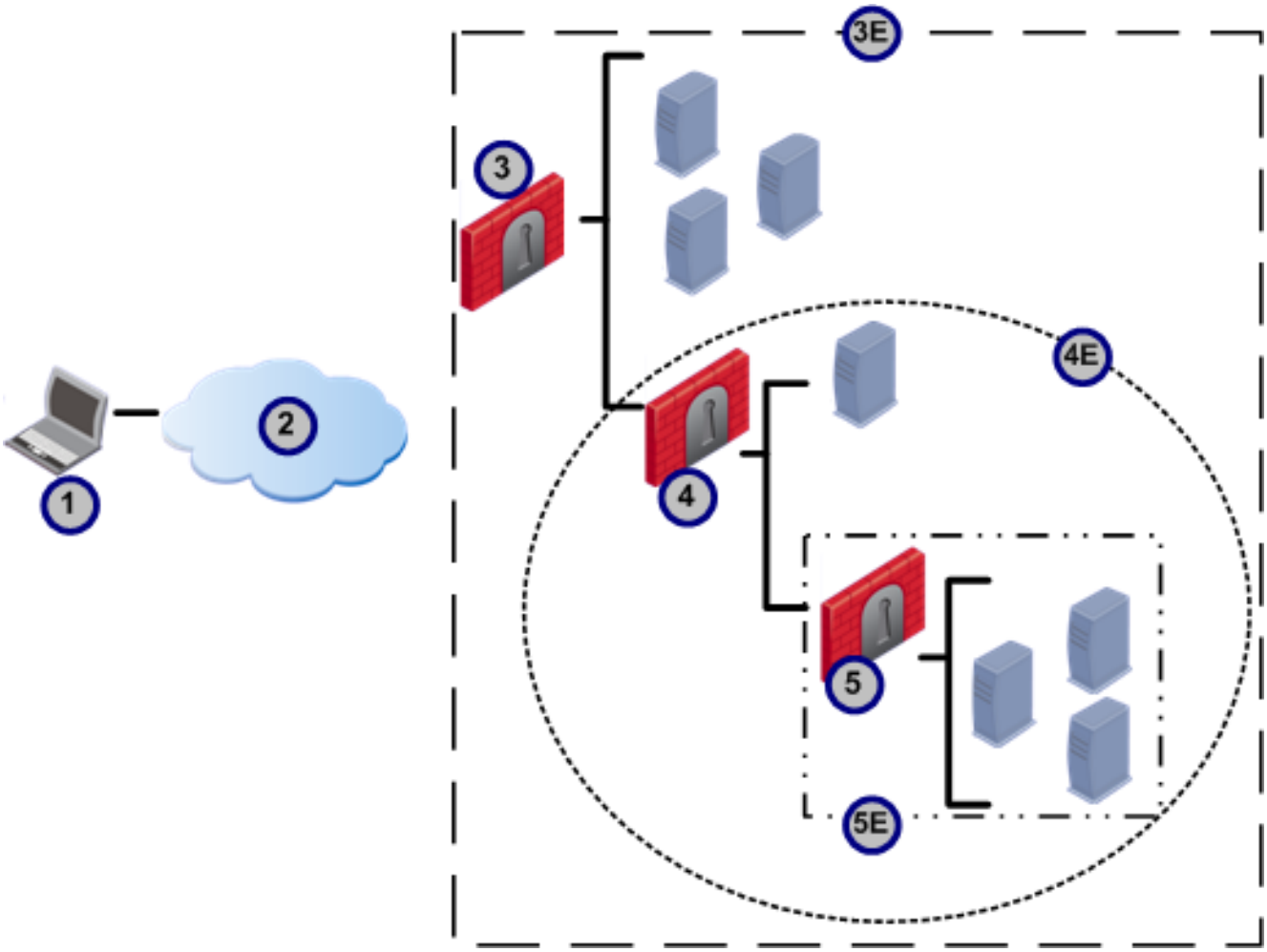


Item	Description
1	Remote Access client
2	Internet

Item	Description
3	Gateway A
3E	Encryption Domain for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B

Remote Access Clients support overlapping encryption domains of this type using Secondary Connect. The client creates an encrypted connection with the Security 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.



Item	Description
1	Remote Access client

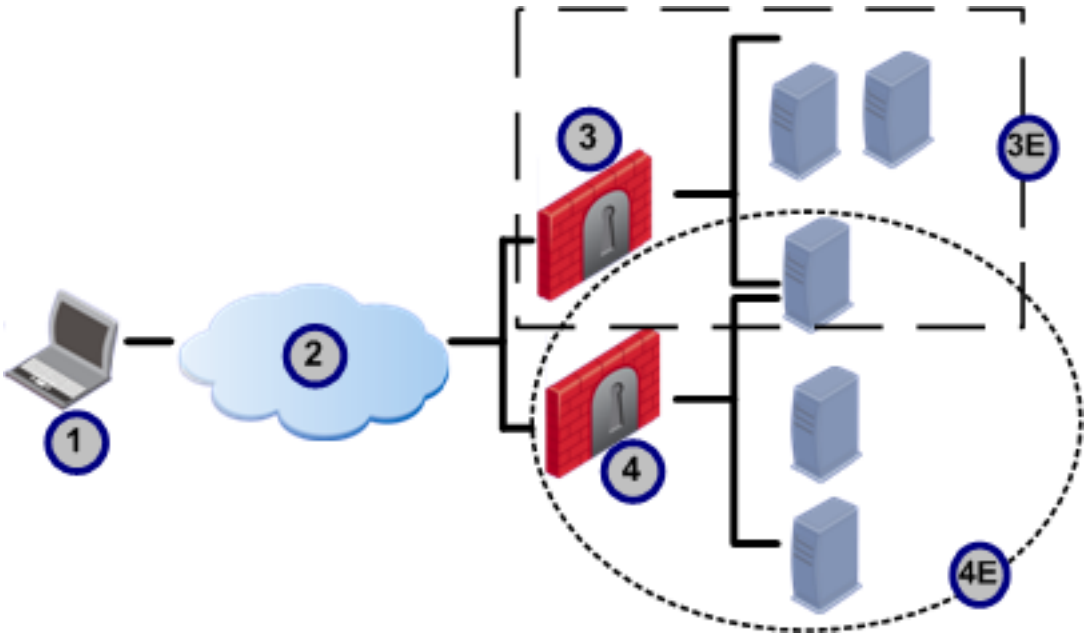
Item	Description
2	Internet
3	Gateway A
3E	Encryption Domain for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B
5	Gateway C
5E	Encryption Domain for Gateway C

The client creates encrypted connections according to these rules:

Host	Connect to:
Hosts in Gateway C's encryption domain	Gateway C
Host only in gateway B's encryption domain and not in another encryption domain	Gateway B
All other hosts	Gateway A

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.

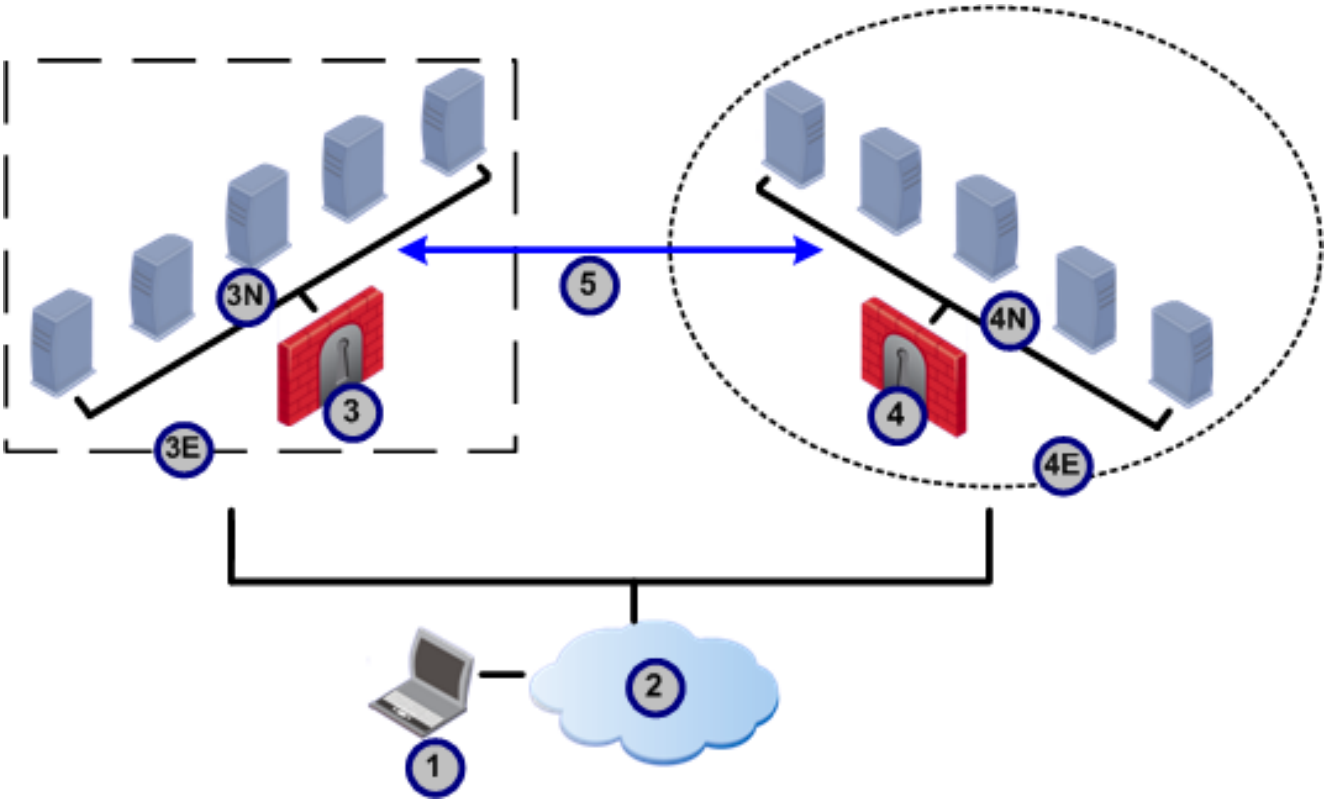


Item	Description
1	Remote Access Client
2	Internet
3	Gateway A
3E	Encryption Domain for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B

Backup Gateways

No Overlapping Encryption Domains

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

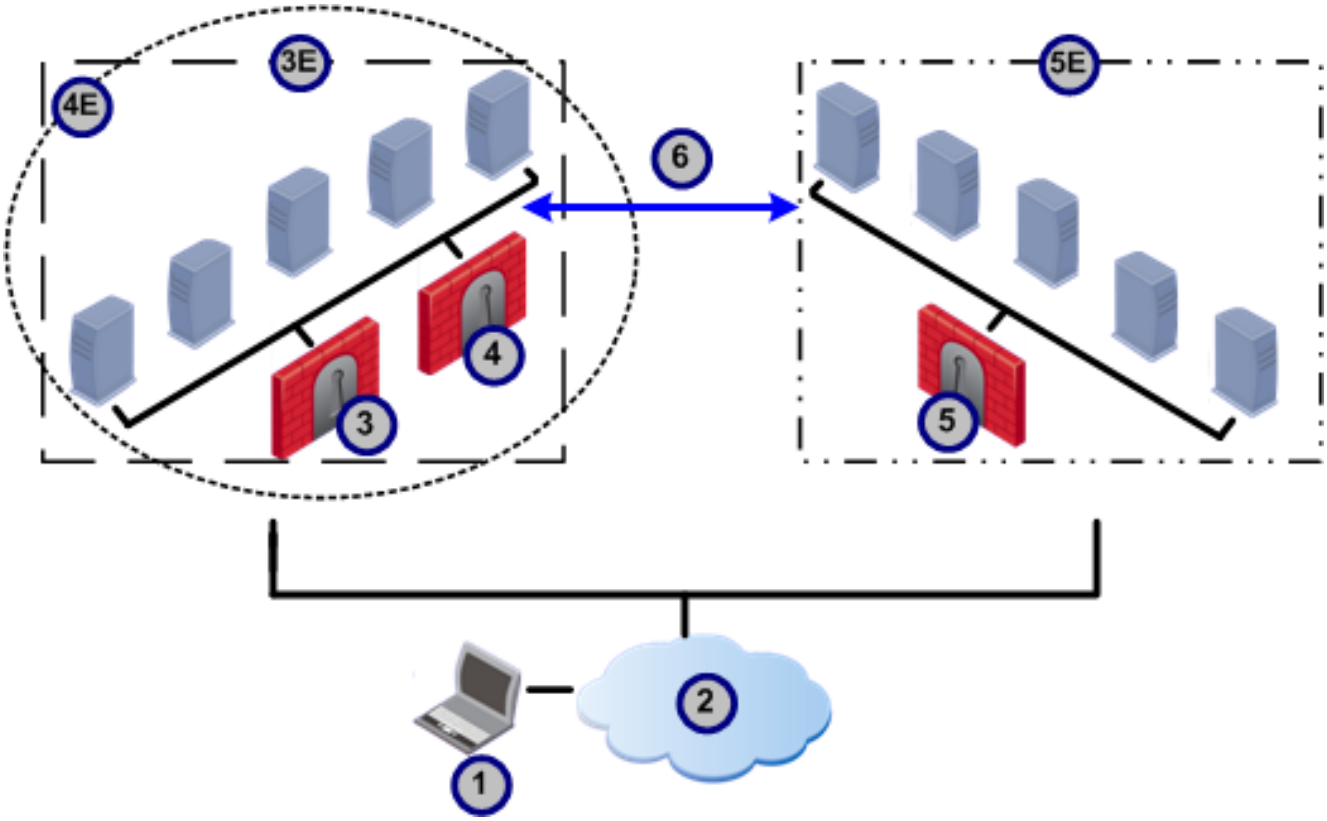


Item	Description
1	Remote Access Client
2	Internet
3	Gateway A
3E	Encryption Domain for Gateway A
3N	Internal Network for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B
4N	Internal Network for Gateway B
5	Dedicated Link

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.



Item	Description
1	Remote Access Client
2	Internet
3	Gateway A
3E	Encryption Domain for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B
5	Gateway C
5E	Encryption Domain for Gateway C
6	Dedicated Link

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.

Creating a DLL file to use with Secure Authentication API

This section describes the technical requirements for a DLL file to use with Secure Authentication API (SAA). 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.

OPSEC - Open Platform for Security

Check Point's OPSEC 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.

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.

Important - 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.

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.

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.

Note - The function prototypes are defined in the file `authplugin.h` which can be found on the OPSEC Desktop SDK.

API Function	Version (Ver)	Summary of Functionality
`PickVersion`	Optional for Ver 1. Required for Ver 2	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.
`RegisterAgent` or `RegisterAgentVer2`	RegisterAgent - Ver 1 RegisterAgentVer2 - Ver 2	Supplies the client with the functions required to work with the Authentication Agent.
`Username`	For Ver 1 and Ver 2	Supplies the username to be used by the client to authenticate with the Security Gateway for SAA Challenge/Response authentication.
`UserNameAndPassword` or `UserNameAndPasswordVer2`	UserNameAndPassword - Ver 1 UserNameAndPasswordVer2 - Ver 2	Supplies the username and password to be used by the client to authenticate with the Security Gateway for SAA Username/Password authentication.

API Function	Version (Ver)	Summary of Functionality
`Response`	For Ver 1 and Ver 2	The client gives the Authentication Agent the challenge that it gets from the Security Gateway. The Authentication Agent returns a response that the client sends back to the gateway the Security Gateway.
`AuthCompleted` or `Terminate`	Terminate - Ver 1 AuthCompleted - Ver 2	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.
`ReleaseContext`	Only for Ver 2	Is called when the client wants to delete context, for example, when a password is expired or has been erased.
`VendorDescription`	For Ver 1 and Ver 2	Returns a meaningful name that the client can display to the user.
`GoingDown`	For Ver 1 and Ver 2	Is called when the client session is going to terminate.
`InvalidateProcCB`	For Ver 1 and Ver 2	Instructs the client to invalidate previous authentications.

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

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

Arguments

Argument	In/Out	Meaning
minVersion	In	Minimum supported client version
maxVersion	In	Maximum supported client version

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

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

Arguments

Argument	In/Out	Meaning
version	In	The version number of the API supported by the client is 2.
Out	The version number of the API supported by the Authentication Agent is 2.	
usernameProc	Out	The address of the Authentication Agent's `UserName` function.
usernameAndPasswordVer2Proc	Out	The address of the Authentication Agent's `UserNameAndPasswordVer2` function.
responseProc	Out	The address of the Authentication Agent's `Response` function.
goingdownProc	Out	The address of the Authentication Agent's `GoingDown` function.
authCompletedProc	Out	The address of the Authentication Agent's `AuthCompleted` function.
releaseContextProc	Out	The address of the Authentication Agent's `ReleaseContext` function.
invalidateProcCB	In	The address of the client callback function that invalidates previous authentication information. The Authentication Agent might call this function to force reauthentication.

Return Values

`PLUGIN_OK` if successful.

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

RegisterAgent

Prototype

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

Arguments

Argument	In/Out	Meaning
version	In	The version number of the API supported by the client is 1.
Out	The version number of the API supported by the Authentication Agent is 1.	
Username	Out	The address of the Authentication Agent's `UserName` function.
usernameAndPassword	Out	The address of the Authentication Agent's `UserNameAndPassword` function.
Response	Out	The address of the Authentication Agent's `Response` function.
Terminate	Out	The address of the Authentication Agent's `Terminate` function.

Argument	In/Out	Meaning
Goingdown	Out	The address of the Authentication Agent's `GoingDown` function.
invalidateProcCB	In	The address of the client callback function that invalidates previous authentication information. The Authentication Agent might call this function to force reauthentication.

Return Values

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

VendorDescription

For versions 1 and 2.

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

Prototype

```
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, but uses it directly.

UserName

`Username` supplies the username to be used by the client to authenticate with the Security 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

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

Arguments

Argument	In/Out	Meaning
site	In	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.
username	Out	The buffer to which `username` should be copied.
usernameLength	In Out	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.
context	Out	A context supplied by the Authentication Agent to be used in subsequent calls to `Response`.

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 canceled.

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 Security 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

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

Arguments

Argument	In/Out	Meaning
site	In	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.
username	Out	The buffer to which `username` should be copied.
usernameLength	In Out	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.
password	Out	The buffer to which the password should be copied.
passwordLength	In Out	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.
context	Out	A context supplied by the Authentication Agent to be used in subsequent calls to `Response`.

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

```
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 Security 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 Security Gateway.

Prototype

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

Arguments

Argument	In/Out	Meaning
context	In	The context as provided by `Username`

Argument	In/Out	Meaning
challenge	Out	The authentication challenge string as received from the Security Management Server.
response	Out	The buffer to which the Authentication Agent's response is to be copied.
usernameLength	In Out	In - Length of the buffer allocated for `response`. 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.

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

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

Arguments

Argument	In/Out	Meaning
context	In	The context as provided by `Username`or `UsernameAndPassWord`.

Argument	In/Out	Meaning
status	In	The status of the authentication. One of these values: ■ `PLUGIN_DONE_SUCCESS` - authentication was successful ■ `PLUGIN_DONE_FAILED` - authentication failed ■ `PLUGIN_DONE` - authentication has been cancelled for example, the password has expired or been erased.
message	In	The termination message, if provided by the authentication server.

Return Values

- `PLUGIN_OK` if successful.
- `PLUGIN_CANCEL` if the input is not correct.

AuthCompleted

For version 2.

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

Prototype

```
int AuthCompleted(void* context, int status, char* message)
```

Arguments

Argument	In/Out	Meaning
context	In	The context as provided by `Username`or `UsernameAndPassWord.`
status	In	The status of the authentication. One of these values: ■ `PLUGIN_DONE_SUCCESS` - authentication was successful ■ `PLUGIN_DONE_FAILED` - authentication failed ■ `PLUGIN_DONE` - authentication has been cancelled for example, the password has expired or been erased.
message	In	The termination message, if provided by the authentication server.

Return Values

- `PLUGIN_OK` if successful.
- `PLUGIN_CANCEL` if the input is not correct.

ReleaseContext

For version 2.

`ReleaseContext` is called when the client wants to delete context, for example, when a password expired or was erased.

Prototype

```
void ReleaseContext(void* context)
```

Arguments

Argument	In/Out	Meaning
context	In	The context as provided by `Username` or `UsernameAndPassWord`.

Return Values

None.

GoingDown

For versions 1 and 2.

The client calls `GoingDown` when the client session is going to terminate.

Prototype

```
void GoingDown()
```

Arguments

There are no arguments.

Return Values

None.

InvalidateProcCB

For versions 1 and 2.

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

Prototype

```
void InvalidateProcCB()
```

Arguments

There are no arguments.

Return Values

None.