

Remote Access Clients for Windows 32/64-bit

E80.41

Administration Guide



23 February 2014

© 2014 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (<http://www.checkpoint.com/copyright.html>) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.

Important Information

Latest Software

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

Latest Documentation

The latest version of this document is at:

(http://supportcontent.checkpoint.com/documentation_download?ID=23222)

To learn more, visit the Check Point Support Center (<http://supportcenter.checkpoint.com>).

For more about this release, see the E80.41 home page

(<http://supportcontent.checkpoint.com/solutions?id=sk91181>).

Revision History

Date	Description
23 February 2014	Updated the note in <i>Using the Command Line</i> (on page 125) Corrected the link to automatic upgrade file in <i>Automatic Upgrade from the Gateway</i> (on page 40) Corrected Remote Access Clients directory paths in <i>Using the Command Line</i> (on page 125) Corrected command syntax in <i>Configuring Secondary Connect</i> (on page 66).
25 June 2013	Added a note in <i>Using Explicit Mode</i> (on page 60)
17 January 2013	First release of this document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments

(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Remote Access Clients for Windows 32/64-bit E80.41 Administration Guide).

Contents

Important Information	3
Introduction to Remote Access Clients	8
Endpoint Security VPN	8
Check Point Mobile for Windows	9
SecuRemote.....	9
Features Overview	9
Connectivity Features in Detail	10
Security Features in Detail	11
Deployment Features.....	12
General Features.....	12
Supported Algorithms and Protocols.....	12
Topology Architecture.....	12
Encryption Domains.....	13
External Resources in Encryption Domain	14
Setting Up Remote Access Clients	15
Workflow for Deploying Clients.....	15
Installing the Remote Access Clients Hotfix.....	16
Required Gateway Settings	16
Configuring a Policy Server.....	22
Creating Installation Package with Administration Mode.....	23
Authentication Schemes and Certificates.....	26
Advanced Client Settings.....	32
Creating Installation Package with VPN Configuration Utility	35
Using the VPN Client Configuration Utility.....	35
Editing an MSI Package with CLI.....	36
Adding Initial Firewall Policy with CLI	39
Installing an MSI Package with CLI.....	39
Distributing MSI Packages.....	40
Automatic Upgrade from the Gateway	40
Configuring Upgrades	41
Endpoint Security VPN for Unattended Machines (ATMs)	41
Configuring the client for ATMs.....	42
Configuring the Client Package.....	42
Deploying the Client Package Manually	43
Using DNS for Automatic Site Detection.....	43
Updating User Sites with the Update Configuration Tool	44
Usage for Update Configuration Tool.....	44
Using the Update Configuration Tool	44
Helping Your Users	46
Simple Installation	46
Remote Access Clients Client Icon.....	46
Helping Users Create a Site	47
Preparing the Gateway Fingerprint	47
Using the Site Wizard	48
Opening the Site Wizard Again.....	49
Helping Users with Basic Client Operations.....	50
Configuring Client Features	52
Intel Smart Connect Technology.....	52
HotSpot Registration	52
Installing Desktop Security Policy	53
Managing Desktop Firewalls.....	53
The Desktop Firewall	54

Rules	54
Default Policy	55
Location-Based Policies.....	55
Allow/Block IPv6 Traffic	56
Logs and Alerts.....	57
Wireless Hotspot/Hotel Registration.....	57
Planning Desktop Security Policy.....	57
Operations on the Rule Base	57
Making the Desktop Security Policy	57
Letting Users Disable the Firewall.....	59
Secure Domain Logon (SDL).....	59
Configuring SDL	59
Configuring Windows Cached Credentials	60
Using SDL in Windows XP.....	60
SDL in Windows Vista and Windows 7	60
Disable or Enable SDL on Internal Network.....	61
Multiple Entry Point (MEP).....	61
Configuring Entry Point Choice	61
Defining MEP Method	62
Implicit MEP.....	62
Manual MEP	64
Making a Desktop Rule for MEP	65
Configuring Geo-Cluster DNS Name Resolution.....	65
Secondary Connect.....	66
Configuring Secondary Connect	66
Secondary Connect for Users	67
Global Properties for Remote Access Clients Gateways	67
Authentication Settings	68
Connect Mode	69
Roaming	69
Location Aware Connectivity.....	69
Idle VPN Tunnel.....	72
Intelligent Auto-Detect.....	73
Smart Card Removal Detection	73
Configuring Hotspot Access.....	74
Split DNS.....	75
Configuring Split DNS	75
Enabling or Disabling Split DNS.....	76
Configuring Log Uploads	76
Configuring Post Connect Scripts	76
Office Mode IP Address Lease Duration.....	77
No Office Mode - Secondary Tunnel Resilience	77
Secondary Tunnel Resilience	77
Secure Configuration Verification (SCV).....	79
Check Point SCV Checks	79
Configuring the SCV Policy	80
Configuring SCV Enforcement.....	80
Configuring SCV Exceptions	81
Traditional Mode.....	81
Installing and Running SCV Plugins on the Client	81
SCV Policy Syntax.....	82
Sets and Sub-sets	82
Expressions	82
Logical Sections.....	83
Expressions and Labels with Special Meanings.....	84
The local.scv Sets.....	85
SCV Parameters.....	86
SCV Global Parameters.....	96
Enforcing the SCV Checks	98

Sample local.scv Configuration File	98
Deploying a Third Party SCV Check	102
The Configuration File	103
Editing the TTM File	103
Centrally Managing the Configuration File	103
Understanding the Configuration File	104
Configuration File Parameters	105
Monitoring and Troubleshooting	106
SmartView Tracker and Remote Access Clients	106
Collecting Logs	107
Remote Access Clients Files	108
"Unsupported Services" Message	109
Configuring No-Router Environments	109
Connection Terminates	110
Troubleshooting the Firewall	110
Using the Windows Service Query	110
Desktop Firewall Monitoring	110
Troubleshooting SCV	117
Traffic Dropped for Anti-spoofing	118
MEP	118
Advanced Configurations	119
Overlapping Encryption Domains	119
Full Overlap	119
Partial Overlap	120
Proper Subset	120
Backup Gateways	122
Remote Access Clients Command Line	125
Using the Command Line	125
CLI Commands	125
change_p12_pwd	125
connect	126
connectgui	127
create	127
delete	127
disable_log	128
disconnect	128
enable_log	128
enroll_capi	128
enroll_p12	129
firewall	129
help	130
hotspot_reg	130
info	130
List	130
Log	131
renew_capi	131
renew_p12	131
set_proxy_settings	132
start	132
stop	133
Ver	133
sdl	133
userpass	133
certpass	134
Creating a DLL file to use with SAA	135
OPSEC - Open Platform for Security	135
Overview of SAA	135
How Does SAA Work	135
Important Note on Working with SAA	136

Summary of OPSEC API Functions.....	136
PickVersion.....	137
RegisterAgent or RegisterAgentVer2	137
RegisterAgentVer2	138
RegisterAgent.....	139
VendorDescription	139
UserName	140
UsernameAndPassword or UserNameAndPasswordVer2	140
UserNameAndPasswordVer2	141
UsernameAndPassword	141
Response	142
Terminate	142
AuthCompleted	143
AuthCompleted	143
ReleaseContext	143
GoingDown.....	144
InvalidateProcCB	144

Chapter 1

Introduction to Remote Access Clients

In This Chapter

Endpoint Security VPN	8
Check Point Mobile for Windows	9
SecuRemote	9
Features Overview	9
Topology Architecture	12

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

The clients offered in this release are:

- **SmartEndpoint-managed Endpoint Security VPN** - The Remote Access VPN blade as part of the Endpoint Security Suite lets users connect securely from their Endpoint Security-protected computer to corporate resources. Clients have the Firewall and Compliance blades managed by SmartEndpoint and other Endpoint Security Software Blades that can be integrated include: Media Encryption & Port Protection, Full Disk Encryption, Anti-Malware, and WebCheck.
- **SmartDashboard-managed clients:**
 - **Endpoint Security VPN** - Incorporates Remote Access VPN with Desktop Security in a single client. It is recommended for managed endpoints that require a simple and transparent remote access experience together with desktop firewall rules.
 - **Check Point Mobile for Windows** - An easy to use IPsec VPN client to connect securely to corporate resources. Together with the Check Point Mobile clients for iPhone and Android, and the Check Point SSL VPN portal, this client offers a simple experience that is primarily targeted for non-managed machines.
 - **SecuRemote** - A secure, yet limited-function IPsec VPN client, primarily targeted for small organizations that require very few remote access clients.

For a detailed feature comparison, see the E80.41 Release Notes *Remote Access Clients E80.41 Release Notes* http://supportcontent.checkpoint.com/documentation_download?ID=23221.

Endpoint Security VPN

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

Check Point Mobile for Windows

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

SecuRemote

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

Features Overview

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

Main Capability	Description
Full IPSec VPN	Internet Key Exchange (version 1) support for secure authentication. A Virtual Private Network (VPN) provides a secured, encrypted connection over the Internet to your organization's network. The VPN tunnel gives remote access users the same security that LAN users have. IPSec makes the tunnel seem transparent because users can run any application or service that you do not block for the VPN. (Compare to SSL VPN, which works through web applications only.)
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 whenever the client exits the internal network.
Proxy Detection	Proxy servers between the client and the gateway are automatically detected and authenticated to if necessary
Dead Gateway Detection	If the client fails to receive an encrypted packet within a specified time interval, it sends a <i>tunnel test</i> packet to the gateway. If the tunnel test packet is acknowledged, the gateway is considered active. If several consecutive tunnel test packets remain unacknowledged, the gateway is considered inactive, or dead. You can configure this feature.
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 gateway protects and gives access to the same VPN domain. MEP lets 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 once to a selected site and get transparent access to resources on different gateways.

Main Capability	Description
Visitor Mode	If the firewall or network limits connections to ports 80 or 443, encrypted (IPSec) traffic between the client and the > is tunneled through a regular TCP connection.gateway.
NAT-T	UDP Encapsulation of IPSec Traffic. Remote Access Clients can connect seamlessly through devices that do not permit native IPSec traffic (such as firewall and access points).
Hub Mode	Increases security. It routes all traffic through the VPN and your gateway. At the gateway, the traffic is inspected for malicious content before being passed to the client, and you can control client connectivity.
VPN Tunneling	Increases connectivity performance. Encrypts only traffic targeted to the VPN tunnel, and let users go more easily to sites where security is not an issue (such as public portals and search engines).
Desktop Firewall	Endpoint Security VPN enforces a Desktop Firewall on SmartDashboard-managed remote clients. The administrator defines the Desktop Security Policy in the form of a Rule Base. Rules can be assigned to either specific user groups or all users; this permits the definition of flexible policies. 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 gateway blocks connectivity for computers that do not comply. It is available in Endpoint Security VPN and Check Point Mobile for Windows. In SmartEndpoint-managed clients, you can choose to use SCV or the Endpoint Security Compliance blade.
Secure Domain Logon (SDL)	Establishes a VPN tunnel before a user logs in.

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.
Multiple Sites	Remote access users can define many gateways to connect to the VPN. If you have multiple VPN gateways, users can try another gateway if the previous one is down or overloaded.
Dialup Support	Endpoint Security VPN supports dial-up connections, useful where a network is not detected.
Hotspot Detection and Registration	Automatically detects hotspots that prevent the client system from establishing a VPN tunnel. Opens a mini-browser to allow the user to register to the hotspot and connect to the VPN gateway.

Feature	Description
Office Mode	Lets a remote client appear to the local network as if it is using a local IP address. This is not supported on SecuRemote
Extended DHCP Parameters	When using Office Mode from a DHCP server, the Remote Access Clients gateway sends data that it got from the client to the DHCP server in the correct format - Hostname, FQDN, Vendor Class, and User Class.
Machine Idleness	Disconnects the VPN tunnel if the machine becomes inactive (because of lock or sleep) for a specified duration.
Keep-alive	Send keep-alive messages from the client to the VPN gateway to maintain the VPN tunnel.
VPN Connectivity to VPN-1 VSX	Terminate VPN tunnel at Check Point VSX gateways.
Split DNS	Support multiple DNS servers.
DHCP Automatic Lease Renewal	Automatically renew IP addresses obtained from DHCP servers

Security Features in Detail

Remote Access Clients support more security features.

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

Deployment Features

Feature	Description
Automatic Client Upgrade from the Gateway	Clients can automatically get an upgrade package when they connect to the gateway. For SmartDashboard-managed clients only.
Pre-configured Client Packaging	You can create a predefined client installation package for easy provisioning.
Localization	Supported languages: <ul style="list-style-type: none"> • Chinese (simplified) - SmartDashboard-managed only • English • French • German • Italian - SmartDashboard-managed only • Japanese • Russian • Spanish

General Features

Feature	Description
Post Connect Scripts	Run a script on client computers after a connection to the gateway is established.

Supported Algorithms and Protocols

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

- 3DES
- AES-128
- AES-256
- MD5
- Sha-1
- Diffie-Helman Group2 (1024)
- Diffie-Helman Group14 (2048)

These transport protocols are supported by Remote Access Clients:

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

Topology Architecture

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

To configure selective routing:

1. In the Network Objects Tree, right click the Security Gateway and select **Edit**.
The **Check Point Security Gateway** properties page opens.
2. Select **Topology** to display the topology window.
3. Click **Set domain for Remote Access Community**.
The **VPN Domain per Remote Access Community** window opens.

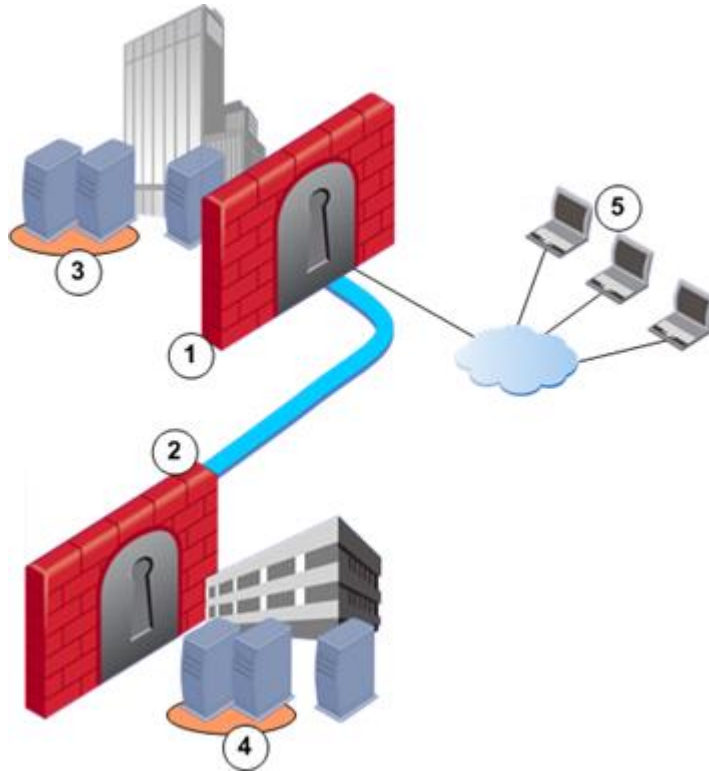
4. Click **Set**.

The **Set VPN Domain per Remote Access Community** window opens.

5. From the drop down menu, select the object that will represent the Remote Access VPN domain.

6. Click **OK**.

Encryption Domains



Scenario 1: Dedicated Encryption Domain

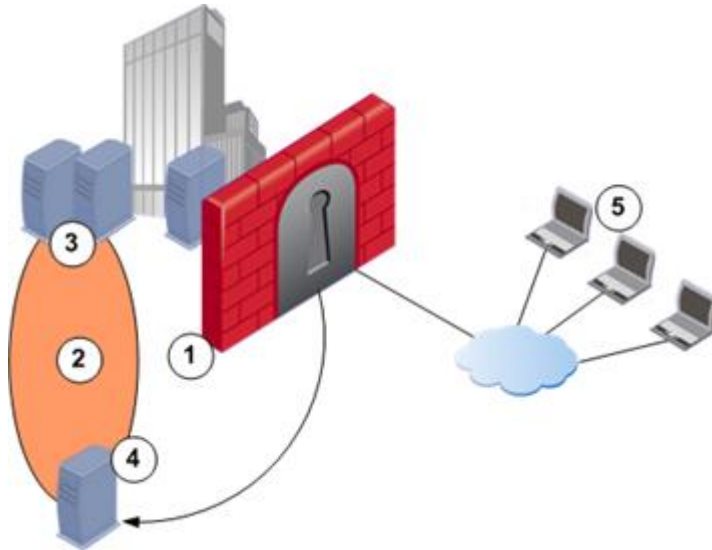
	Component	Connects To
1	Gateway of Site 1	<ul style="list-style-type: none"> Gateway of Site 2 in site-to-site VPN Remote Access Clients, as their VPN gateway
2	Gateway of Site 2	Gateway of Site 1 in site-to-site VPN
3	Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 2
4	Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 1
5	Remote Access Clients	<ul style="list-style-type: none"> 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
1	Gateway of Site 1	<ul style="list-style-type: none"> 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
2	Gateway of Site 2	Gateway of Site 1 in site-to-site VPN
3	Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 2

	Component	Connects To
4	Servers in Remote Access Encryption Domain	Servers in Encryption Domain of Site 1
5	Remote Access Clients	<ul style="list-style-type: none"> Gateway of Site 1 through encrypted VPN Permitted servers (3 and 4) <p>Note - clients can reach servers of two sites with one authentication session, and their activity in both sites is logged</p>

External Resources in Encryption Domain



	Component	Connects To
1	Gateway of Site 1	<ul style="list-style-type: none"> Remote Access Clients, as their VPN gateway (5) External resource (4) Redirects clients (5) to external resource (4)
2	Remote Access Encryption Domain	Encrypted domain of gateway (1) that includes an external resource
3	Servers in Encryption Domain	External resource
4	External (Internet or DMZ) resource in Encryption Domain	<ul style="list-style-type: none"> Server in Encryption Domain Remote Access Clients if the gateway redirects
5	Remote Access Clients	<ul style="list-style-type: none"> Gateway of Site 1 through encrypted VPN Permitted servers (3) External resource (4), through gateway redirect

Chapter 2

Setting Up Remote Access Clients

In This Chapter

Workflow for Deploying Clients	15
Installing the Remote Access Clients Hotfix	16
Required Gateway Settings	16
Creating Installation Package with Administration Mode	23
Creating Installation Package with VPN Configuration Utility	35
Editing an MSI Package with CLI	36
Distributing MSI Packages	40
Automatic Upgrade from the Gateway	40
Endpoint Security VPN for Unattended Machines (ATMs)	41
Using DNS for Automatic Site Detection	43
Updating User Sites with the Update Configuration Tool	44

Workflow for Deploying Clients

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

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

The initial workflow includes:

1. Install the gateway Hotfix, if required.
2. Configure the gateway.
3. Download a client package and edit the package, if necessary.

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

 - a) **SmartEndpoint-managed Remote Access VPN** - Use the VPN Configuration Utility ("[Creating Installation Package with VPN Configuration Utility](#)" on page 35).
 - b) **SmartDashboard-managed Remote Access Clients** - You can use these tools to edit the client MSI:
 - The VPN Configuration Utility ("[Creating Installation Package with VPN Configuration Utility](#)" on page 35).
 - Client application in Administration Mode ("[Creating Installation Package with Administration Mode](#)" on page 23).
 - CPMSI Tool with CLI. ("[Editing an MSI Package with CLI](#)" on page 36)
4. Distribute the package.
 - Through GPO or email, using the MSI file.
 - Distribute an upgrade automatically from the 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.

Installing the Remote Access Clients Hotfix

Install the Endpoint Security VPN R75/Remote Access Clients E80.41 Hotfix on gateways or standalone, self-managed gateway deployments. To use Automatic MEP, install the hotfix on all gateways and the Security Management Server. In a Multi-Domain Security Management environment install the hotfix on the Multi-Domain Server.

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

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

The Remote Access Clients Hotfix enables NGX R65.70 and R70.40 gateways to support E80.41 Remote Access Clients.

Before you install the Hotfix:

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

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

1. Download the Remote Access Clients Hotfix.
2. Copy the Hotfix package to the Security Gateway or Security Management Server.
3. Run the Hotfix:

On SecurePlatform, Disk-based IPSO, and Solaris:

- a) `tar -zxvf <name_of_file>.tgz`
- b) `./UnixInstallScript`

On Windows platforms: double-click the installation file and follow the instructions.

4. Reboot the Security Gateway or Security Management Server.

To install the Hotfix on a Multi-Domain Server:

1. On the Multi-Domain Server, run: `mdsenv`.
2. Download the Remote Access Clients Hotfix from sk65209 (<http://supportcontent.checkpoint.com/solutions?id=sk65209>) to the Multi-Domain Server.
3. Run the Hotfix on SecurePlatform and Solaris:

- a) `tar -zxvf <name_of_file>.tgz`
- b) `./UnixInstallScript`

4. Follow the on-screen instructions.
5. Reboot the Multi-Domain Server.

Required Gateway Settings

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



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

To configure Remote Access Clients management on the gateway:

1. In SmartDashboard, right click the gateway and select **Edit**.
The **Check Point Gateway** window opens.
2. Configure remote VPN functionality:
 - R70 and higher: In the **General Properties** page, enable the **IPSec VPN** blade.

Check Point Gateway - General Properties

Machine

Name: Color:

IP Address:

Comment:

Secure Internal Communication

State:


Platform

Hardware: Version: OS:

Software Blades

Network Security Blades: Management Blades:

Network Security (5) Management (4)

<input checked="" type="checkbox"/> Firewall <input checked="" type="checkbox"/> IPSec VPN <input type="checkbox"/> Policy Server <input type="checkbox"/> Mobile Access <input checked="" type="checkbox"/> IPS <input checked="" type="checkbox"/> URL Filtering <input type="checkbox"/> Anti-Virus & Anti-Malware <input type="checkbox"/> Anti-Spam & Email Security <input type="checkbox"/> Data Loss Prevention <input checked="" type="checkbox"/> Monitoring	<p>Advanced Networking</p> <input type="checkbox"/> QoS Dynamic Routing <input type="button" value="i"/> ConnectControl <input type="button" value="i"/> <p>Acceleration & Clustering</p> SecureXL <input type="button" value="i"/> <p>More</p> <input type="checkbox"/> FireWall-1 GX <input type="checkbox"/> UserAuthority Server <input type="checkbox"/> UserAuthority WebAccess	<p>Firewall</p> <p>World's most proven firewall solution that can examine hundreds of applications, protocols and services out-of-the box.</p>  <p>More Info <input type="button" value="v"/></p>
--	---	--

- NGX R65: In the **General Properties** page > **Check Point Products**, select **VPN**.



Note - This is for all IPSec VPN functionality, not just Remote Access Clients.

3. Add the gateway to the **Remote Access VPN** community:

- R71 and higher: Open **IPSec VPN** and click **Add**.

- General Properties
- Topology
- NAT
- IPS
- IPSec VPN**
- Authentication
- Monitoring Software bl.
- Logs and Masters
- Capacity Optimization
- Cooperative Enforcem
- Advanced

IPSec VPN

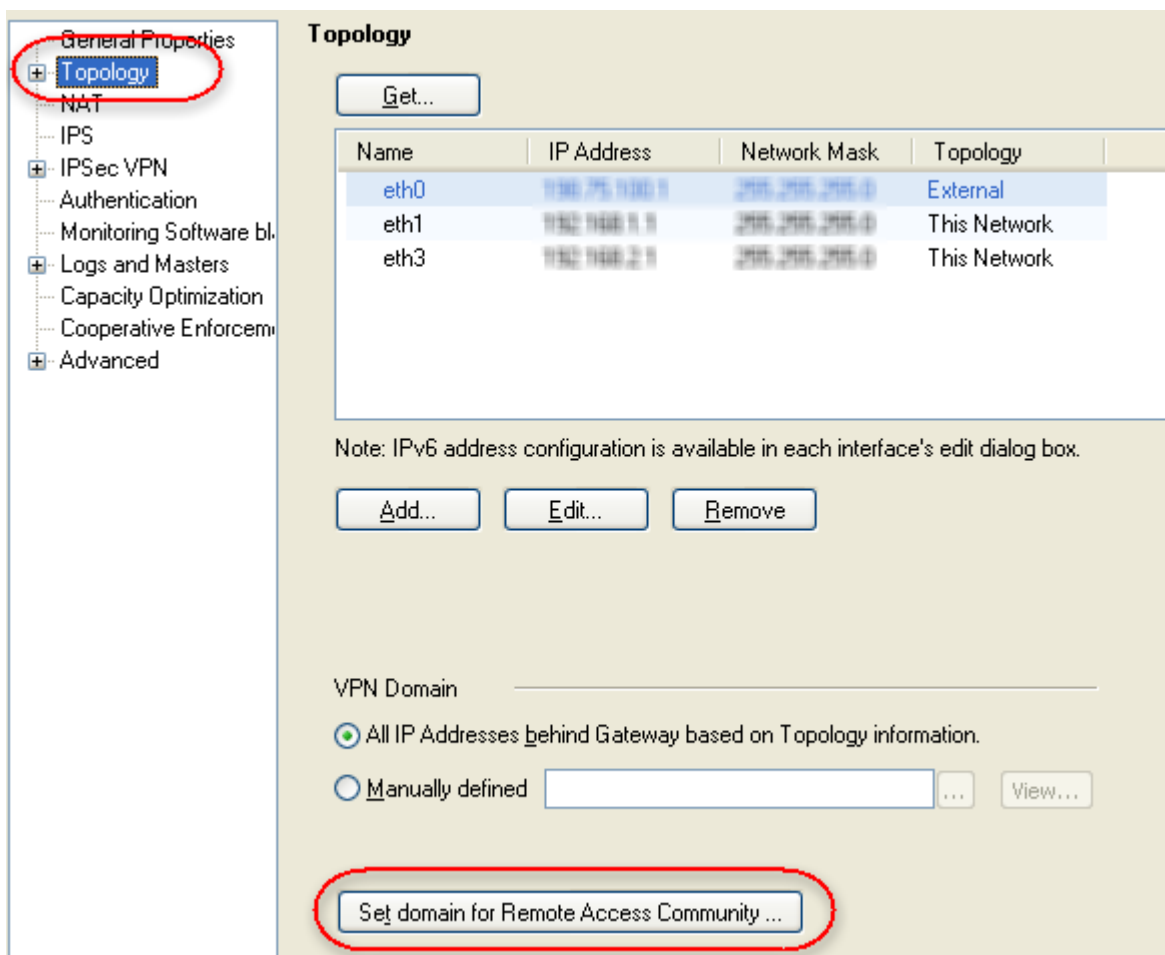
This Security Gateway participates in the following VPN Communities:

- NGX R65 / R70: Open **VPN** and click **Add**.

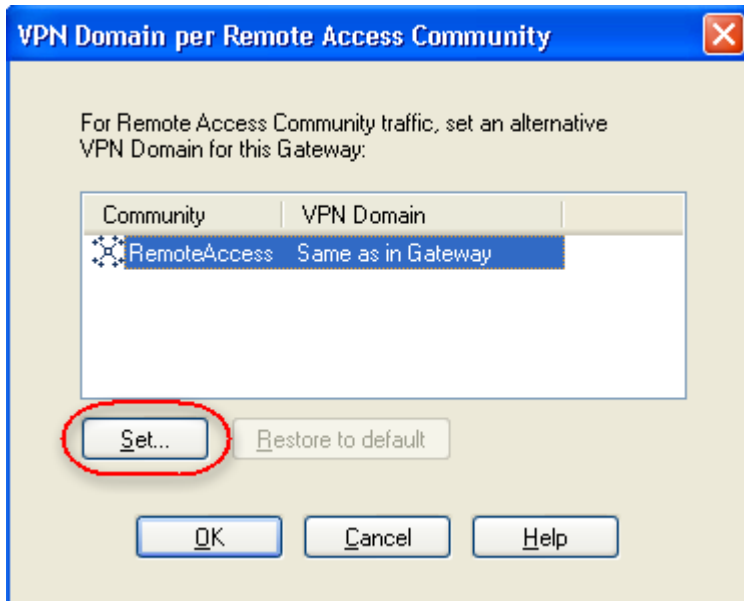
In the window that opens, click **Remote Access** and click **OK**.



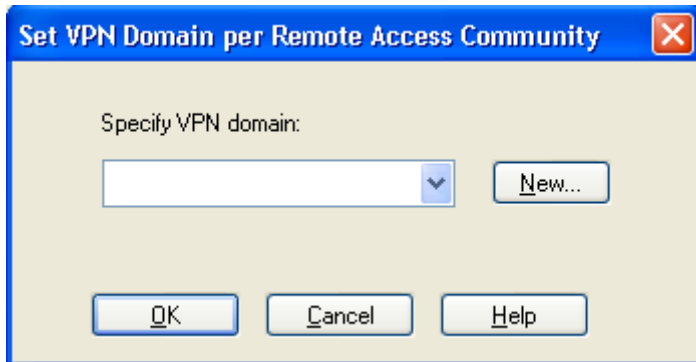
4. Set the VPN domain for the Remote Access community.
 - a) Open **Topology** and click **Set domain for Remote Access Community**.



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



- c) In the window that opens, select a VPN Domain and click **OK**, or click **New** and define a VPN domain.



- d) Click **OK**.

5. Configure **Visitor Mode**.

- R71 and higher: Open **IPSec VPN > Remote Access**.
- NGX R65 / R70: Open **Remote Access**.

Select **Visitor Mode** and leave **All Interfaces** selected. You can choose the Visitor Mode **Service**, which defines the protocol and port of Endpoint Security VPN connections to the gateway.

Remote Access

L2TP Support _____

Support L2TP (relevant only when Office Mode is active)

Authentication Method: Smart Card or other Certificate (encryption e... ▾

Use this certificate: _____ ▾

Hub Mode configuration _____

Allow SecureClient to route traffic through this gateway

NAT traversal (Check Point proprietary) _____

Support NAT traversal mechanism (UDP encapsulation)

Allocated port: UDP VPN1_IPSEC_encapsulation ▾

Visitor Mode configuration _____

Support Visitor Mode

Service: TCP https ▾

Machine's Interface: All Interfaces ▾

6. Open **Office Mode** and select **Office Mode**.

Office Mode

Do not offer Office Mode

Offer Office Mode to group: L2TP-vpn-user ▾ New...

Allow Office Mode to all users

Office Mode Method _____

Allocate IP address by sequentially trying the checked methods, until success:

From ipassignment.conf located in \$FWDIR/conf - always tried first

From the RADIUS server used to authenticate the user

Using one of the following methods:

Manual (using IP pool)

Allocate IP addresses from network: Remote-1-dmz ▾

Automatic (using DHCP)

Use specific DHCP server: _____ ▾ New...

Virtual IP address for DHCP server replies: _____

MAC address for DHCP allocation: Unique per machine ▾

Optional Parameters...

- Select for a group or for all users.
- Select an Office Mode method.
- Click **OK**.



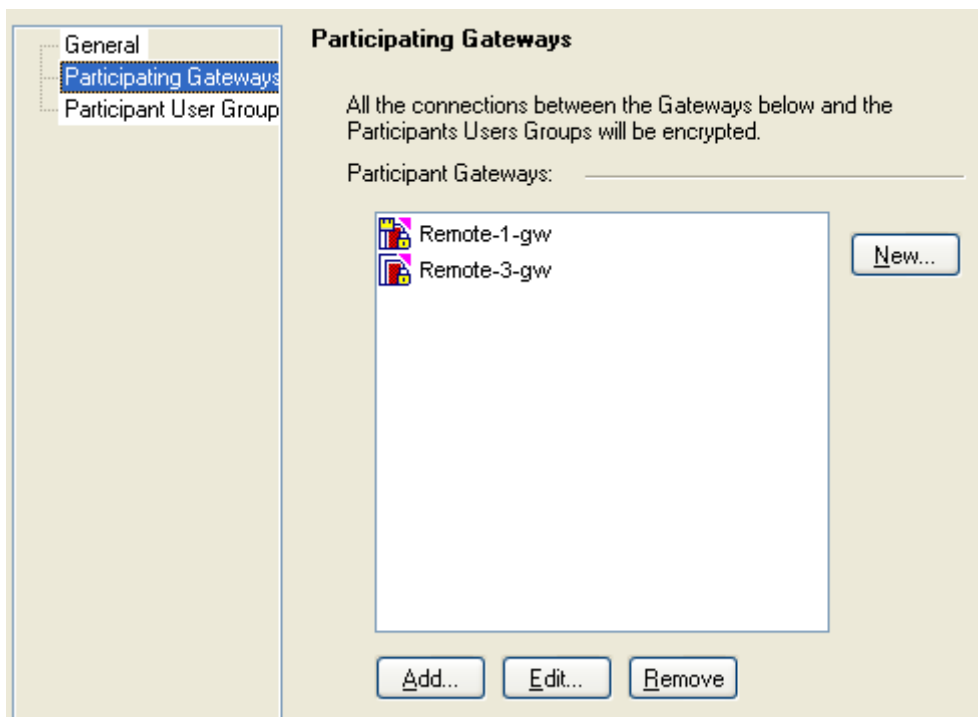
Note - Office mode is not supported in SecuRemote. If you use SecuRemote, you can select **Do not offer Office Mode**. If another option is selected, it is ignored.

To add Remote Access Clients users to the VPN:

1. Open the Remote Access Community Properties window:
 - R70 and higher: Open the **IPSec VPN** tab on SmartDashboard.



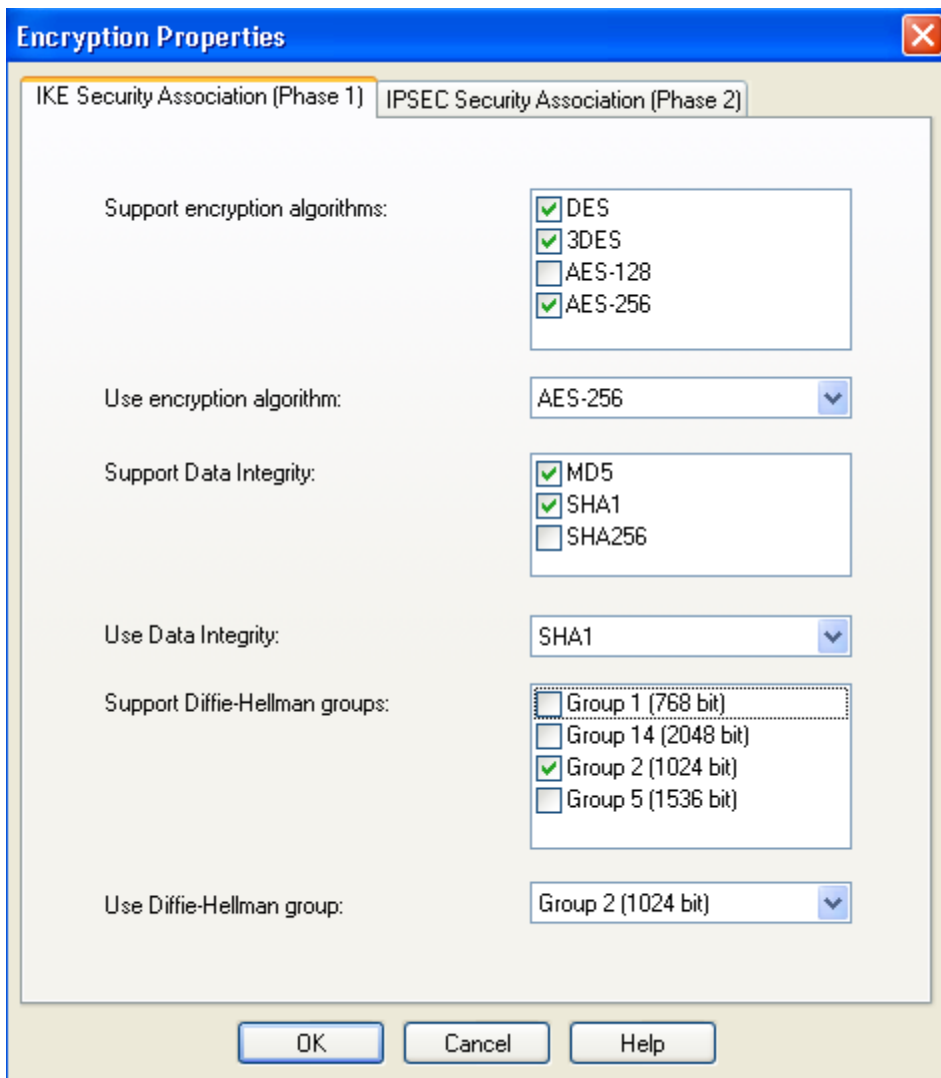
- NGX R65: Open the **VPN** tab on SmartDashboard.
2. Double-click the **Remote Access VPN** community.



3. Open **Participant User Groups**. Make sure all Remote Access Clients client users are added.
 - You can leave **All Users**.
 - You can click **Add** to add existing user groups to the community.
 - You can click **New** to create a new user group or add an LDAP group.
4. Open **Participating Gateways**. Make sure the gateway you want to manage Endpoint Security VPN clients is listed.
5. Close **OK**.

To configure encryption for the VPN:

1. Open **Policy** menu > **Global Properties**.
2. Open **Encryption Properties**.
 - R71 and higher: Open **Remote Access** > **VPN - Authentication and Encryption** and click **Advanced**.
 - NGX R65 / R70: Open **Remote Access** > **VPN - IKE (Phase 1)**.



3. In the **Support encryption algorithms** list, make sure that at least one **AES** encryption algorithm is selected.
4. In the **Use encryption algorithm** list, select an enabled AES encryption algorithm.



Important - The client does not support DES algorithms. You *must* select an AES algorithm.

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

Configuring a Policy Server

This applies to SmartDashboard-managed Endpoint Security VPN and Check Point Mobile for Windows.

The Policy Server functionality in a gateway is the Desktop Security Policy management. If you do not enable a Policy Server, the Desktop rule base and the SCV checks will not be applied.

To define a gateway as the Policy Server:

1. In SmartDashboard, right-click the gateway that will serve as the Policy Server and select **Edit**. The **Check Point Gateway** window opens.
2. Enable Policy Server functionality:
 - R70 / R71: In **Software Blades > Network Security**, click **IPSec VPN** and **Policy Server**.
 - NGX R65: In **Check Point Products**, click **VPN** and **SecureClient Policy Server**.

3. Open Authentication.

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

Remote Access Modes

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



Note - Hub mode is not supported in SecuRemote.

To enable Hub Mode:

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

Creating Installation Package with Administration Mode

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

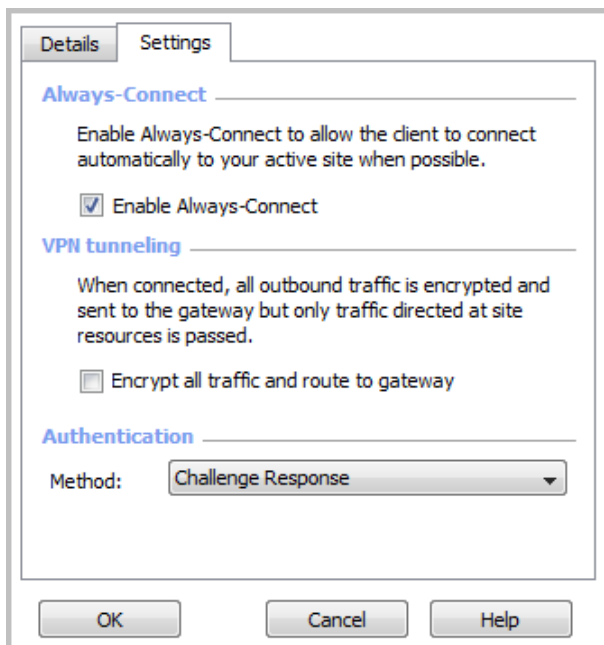
- Which client installs (Endpoint Security VPN, Check Point Mobile for Windows, or SecuRemote)
- A VPN site
- The authentication method
- An initial firewall policy



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

To create a pre-configured package:

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



8. Configure the VPN options:
 - **Always-Connect** - Let the client connect automatically to the active site.
 - **VPN tunneling** - Make sure the client connects to the VPN for all outbound traffic. Enable Hub Mode for the gateway ("[Remote Access Modes](#)" on page 23).
 - **Authentication** ("[Authentication Schemes and Certificates](#)" on page 26)
9. Click **OK**.
10. Select the **Advanced** tab and configure settings ("[Advanced Client Settings](#)" on page 32) as required for your environment.

11. Select the **Administration** tab.

The screenshot shows the 'Administration' tab in the Check Point Endpoint Security console. The 'Packaging' section is active, featuring an 'Input MSI Package Path' text box with a 'Browse...' button to its right. Below this are three checkboxes: 'Replace user's configuration when upgrading' (unchecked), 'Enforce default firewall policy after client installation' (unchecked), and 'Select a product:' (checked). Under 'Select a product:', there is a note: '(if you do not select a product, it will have to be selected during the installation)'. Three radio buttons are listed: 'SecuRemote' (unchecked), 'Check Point Mobile' (unchecked), and 'Endpoint Security VPN' (checked). A 'Generate' button is located at the bottom of the packaging section. At the very bottom of the console window, there are 'Close' and 'Help' buttons.

- a) **Input MSI Package Path** - Click **Browse** and select the input MSI package file.
- b) **Replace user's configuration when upgrading** -
 - When cleared, users keep their configuration after the upgrade.
 - When selected, the new configuration is merged with the old configuration. Users do not have to apply for new credentials to a site that they have been using.
- c) **Enforce default firewall policy after client installation** -
 - When cleared, clients that install Endpoint Security VPN only enforce a firewall policy after they connect to the VPN for the first time.
 - When selected, when Endpoint Security VPN is installed it will immediately enforce the initial firewall policy. The initial firewall policy is the last policy installed on the computer where the MSI is generated at the time that it is generated. It is enforced until the client connects to the VPN and gets a different policy.
- d) For new installations, select a product that users install: Endpoint Security VPN, Check Point Mobile for Windows, or SecuRemote.
 If you do not select a product, users can choose.
 If users already have an E75.x Remote Access Client installed, this will not change the product type.
- e) Click **Generate** to create the MSI package.
 A window opens to select a location to save the generated package.

12. Distribute this package to Remote Access Clients users.

13. Users will double-click the MSI file and follow the on-screen instructions.



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

Authentication Schemes and Certificates

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

Remote Access Clients support these authentication types:

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

Pre-Configuring Authentication Method

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

To change the authentication scheme from the client:

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

If you do not want to pre-package the MSI, you can pre-configure the default authentication method in the gateway configuration file.

To configure default authentication for users of a site:

1. On the gateway, open the `$FWDIR/conf/trac_client_1.ttm` file with a text editor.
2. In the `default_authentication_method` section, change `:default`
Valid values:
 - `client_decide` (let user decide, default)
 - `username-password`
 - `certificate` (for Certificate “CAPI”)
 - `p12-certificate`
 - `securIDKeyFob`
 - `securIDPinPad`
 - `SoftID`
 - `challenge-response`
 - `SAA-username-password`
 - `SAA-challenge-response`
3. Save the file and install the policy.
When clients download the new policy from the gateway, configuration changes are applied.

This example shows a configuration for Certificate - P12 authentication.

```

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

```

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

Certificates

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

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

Stored in CAPI or Stored as Files

Remote Access Clients support user authentication through **PKCS#12** certificates. A **PKCS#12** certificate can be accessed directly when stored as a **.p12** file or imported to the CAPI store.

CAPI lets Windows-based applications do cryptographic operations. The CAPI *store* is a repository of digital certificates associated with a Cryptographic Service Provider (CSP). Each CSP controls the cryptographic keys belonging to the certificates.

Decide whether to let users import certificates to the CAPI store:

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

Generating and Deploying Certificates

Generate certificates in SmartDashboard:

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

Generating Registration Keys

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

To generate a registration key:

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

Generating PKCS#12 Files

Generate a certificate file from SmartDashboard.

To generate a certificate file:

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

Certificate Enrollment and Renewal

The minimum P12 certificate password length is 4 characters. If users enter a shorter password, an error message shows and they are prompted to enter a longer password. The minimum length can be changed in the TTM file. See sk75221 (<http://supportcontent.checkpoint.com/solutions?id=sk75221>) for the parameters.

A. To enroll a certificate:

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

B. To renew a certificate:

1. Right-click the client icon in the system tray, and select **VPN Options**.
2. On the **Sites** tab, select the site from which you will renew a certificate and click **Properties**.
The site **Properties** window opens.
The authentication method you chose is set and the certificate will be renewed accordingly.
3. Select the **Settings** tab.
4. Click the **Renew** button.
The **CAPI** or **P12** window opens.

5. For CAPI, choose the certificate you want to renew from the drop-down list. For P12, choose a P12 file and enter its password.
6. Click **Renew**.
The certificate is renewed and ready for use.

Revoking Certificates

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

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

Helping Users Import Certificates to CAPI Store

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

To import a certificate through the client:

1. Right-click the client icon, and select **VPN Options**.
2. On the **Sites** tab, select the gateway and click **Properties**.
3. Open the **Settings** tab.
4. Make sure that **Certificate - CAPI** is selected in the **Method** menu.
5. Click **Import**.
6. Browse to the P12 file.
7. Enter the certificate password and click **Import**.

To import a certificate through Windows file explorer:

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

Disabling CAPI Authentication

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

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

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

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

3. Save the file and install the policy.

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

SecurID

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

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

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

SoftID

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

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

Key Fobs

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

Working with RSA Hard and Soft Tokens

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

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

To configure RSA SoftID:

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

Secure Authentication API (SAA)

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

You select Secure Authentication API (SAA) as the authentication method when you create a site or when you create an MSI package. You then select a DLL file to use. The DLL is a file that you create that uses the

OPSEC API and other SAA API to interface with the client. When users connect to a site, a window opens based on the SAA authentication type that is configured for the site, and users authenticate seamlessly.

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



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

For details of how to create the required DLL file, see [Creating a DLL file to use with SAA](#) (on page 135).

Configuring SAA

You can configure SAA in these ways:

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

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

To configure SAA for an installation package:

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

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

To configure SAA as the authentication method for a site:

1. From the Site Wizard, on the **Authentication Method** page, select **Secure Authentication API (SAA)**. A **Secure Authentication API (SAA)** page opens.

Secure Authentication API (SAA)
Select the type of third party authentication that you use.

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

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

Use a Secure Authentication API File:
<Select a SAA DLL file>

Select the Secure Authentication API DLL file supplied by your administrator. If you do not have this, contact your administrator.

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

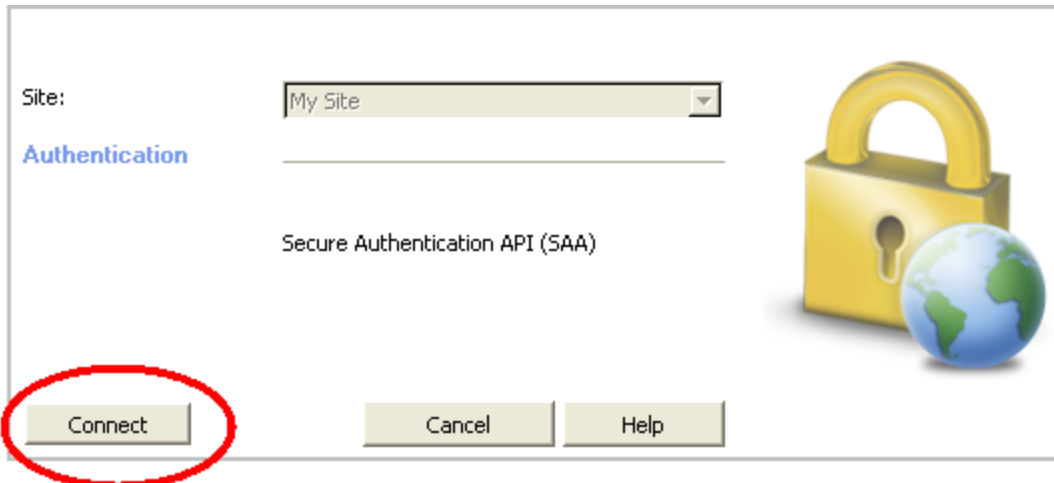


Note - Only users with administrator permissions can replace the DLL.

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

SAA From the User's Perspective

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



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

Challenge-Response

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

Authentication Timeout

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

To change Authentication Timeout:

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

Advanced Client Settings

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

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

2. Open the **Advanced** tab.

Pre-Configuring Logging Options

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

To define a default email address for log files:

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

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

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

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

Pre-Configuring Proxy Settings



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

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

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

To configure proxy settings on the client:

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

The **Proxy Settings** window opens.

The screenshot shows the 'Proxy Settings' dialog box with the following details:

- Proxy Definition:**
 - No proxy (selected)
 - Detect proxy from Internet Explorer settings
 - Manually define proxy
- Manually define proxy fields:**
 - Address: [Empty text box]
 - Port: [8080]
- Proxy Authentication:**
 - Username: [Empty text box]
 - Password: [Empty text box]
- Buttons:** OK, Cancel, Help

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

Configuring Client Interface Language

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

To change the interface language:

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

Pre-Configuring SDL Enable

You can enable SDL ("[Secure Domain Logon \(SDL\)](#)" on page 59) for the Remote Access Clients.

To enable SDL in the client:

1. Open the **Options > Advanced** tab.
2. Click **Enable Secure Domain Logon**.

Replacing the DLL File

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



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

To replace the local DLL file:

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

Creating Installation Package with VPN Configuration Utility

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

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

The VPN Configuration Utility gives you these options:

- Replace the Trac.config and Trac.defaults files that users install as part of the client MSI.
 - The Trac.config file includes the site configuration
 - The Trac.defaults file
- Enable Secure Domain Logon
- Enable using fixed MAC addresses for Office Mode IP allocation.
- Choose which client type to install (SmartDashboard-managed only).
- Add SCV plugins.

Using the VPN Client Configuration Utility

Get the VPN Client Configuration Utility, **VPNConfig.exe**, from:

sk91181 (<http://supportcontent.checkpoint.com/solutions?id=sk91181>)

Or as part of the SmartConsole installation files:

32 bit: C:\Program Files\CheckPoint\SmartConsole\E80.40\PROGRAM\data\RepWorkFolder\VPNConfigTool

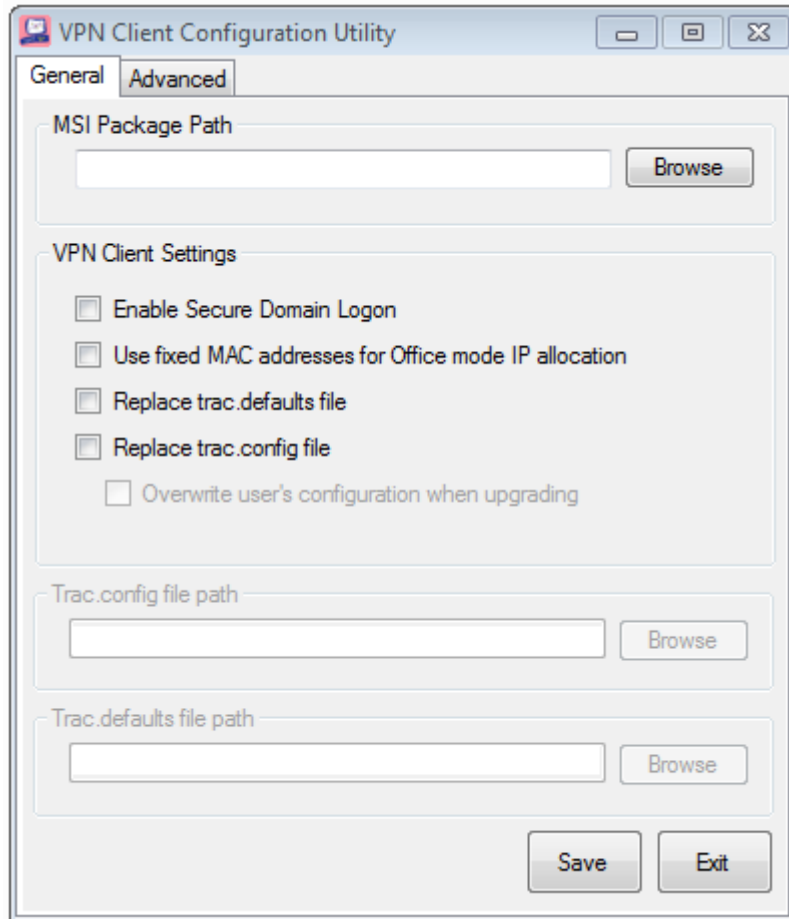
64 bit: C:\Program Files
(x86)\CheckPoint\SmartConsole\E80.40\PROGRAM\data\RepWorkFolder\VPNConfigTool

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

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

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

The VPN Client Configuration Utility opens.



3. Click **Browse** to select the location of the MSI.
4. Select the options to include in the MSI:
 - **Enable Secure Domain Logon**
 - **Use fixed MAC addresses for Office mode IP allocation**
 - **Replace trac.defaults file**
 - **Replace trac.config file**
5. If you selected to replace a trac file:
 - 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 files are overwritten by the new trac files.
 - Browse to the path of the trac files that you want to include. If you replace the trac.config file you have to provide the path for both trac.config and trac.defaults.
6. Optional: Open the **Advanced** tab.
 - For SmartDashboard-managed clients, select a **VPN Client sub type**:
 - **Endpoint Security VPN**
 - **Check Point Mobile for Windows**
 - **SecuRemote**
 - Click **Add** to add **SCV Plugins**.
7. Click **Save**.
8. Select the location where the new MSI will be saved.

Editing an MSI Package with CLI

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

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

Syntax

```
package-package-file-name>  
[<-in|-out|-add|-overwrite|-overwrite|-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 <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: <ul style="list-style-type: none"> LangPack1.xml DisconnectedPolicy.xml Trac.config
-out	Remove <filename> from the package. The file can be a filename from the list below, or "all" for all of them. The file must exist in same directory as the MSI file. Possible files: <ul style="list-style-type: none"> LangPack1.xml DisconnectedPolicy.xml Trac.config
-add	Add <filename> to the package. The file can be any file. It must exist in same directory as the MSI file.
-remove	Remove a file <filename>, that you added previously, from the MSI.
-overwrite	Overwrite <filename> with a new version of the file. It must be a file that was added.
-copyout	Save <filename> as a separate file.
-add_scv_plugin	Add a third party SCV plugin file to the package. <filename> is the name of the SCV plugin. The file must exist in same directory as the MSI file.
-remove_scv_plugin	Remove a third party SCV plugin file from the package. <filename> is the name of the SCV plugin.
-overwrite_scv_plugin	Overwrite a third party SCV plugin file that was added to the package previously.
-replace_config	Previously: nk Possible values: true or false true - When a user upgrades the client with this MSI, the user site list is replaced but his personal data is kept. This is done by merging the old trac.config and new trac.config files. false - When a user upgrades the client with this MSI, the old user trac.config file is kept and is not replaced by the new trac.config file from the installation.
-sdl_enable	Enable SDL Possible values: true or false true - Secure Domain Logon (SDL) is enabled for the package.
-fixed_mac	Possible values: true or false true - The client will use fixed Office mode MAC addresses.
-ClientSubType	Default client type. Possible values: SecuRemote CheckPointMobile EndpointSecurityVpn UserDecide



Note - `DisconnectedPolicy.xml` is on client computers in:

- Windows Vista and higher - `C:\Windows\System32\drivers`
- Windows XP - `C:\Windows\System32`

LangPack1.xml is on client computers in the installation directory:

- 32 bit - `C:\Program Files\CheckPoint\Endpoint Connect`
- 64 bit - `C:\Program Files (x86)\CheckPoint\Endpoint Connect`

Adding Initial Firewall Policy with CLI

An initial firewall policy is the last policy installed on the computer where the MSI is generated. It is enforced until the client connects to the VPN and gets a different policy. For SmartDashboard-managed clients, you can add an initial firewall policy to be enforced after installation

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

- `DisconnctedPolicy.xml`
- `desktop_policy.ini`



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

To add the files required for an initial firewall:

```
Run: cpmsi_tool -in DisconnctedPolicy.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.	<code>"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qb! INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect"</code>	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.	<code>"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qb! INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect"</code>	qb! No user interaction is required
No User Interface - All user interface is hidden.	<code>"C:\WINDOWS\system32\msiexec.exe" /i "C:\Program Files\CheckPoint\Endpoint Connect\CheckPointEndpointSecurity.msi" /qn INSTALLDIR="C:\Program Files\CheckPoint\Endpoint Connect"</code>	qn - no UI

Distributing MSI Packages

You can distribute MSI files to users in different ways:

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

Users must have administrator privileges to install the MSI.

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

Some examples of client deployment options are:

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

Automatic Upgrade from the Gateway

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

If you have a gateway version that requires the Remote Access Clients Hotfix, make sure that the Hotfix is installed before you put an upgraded package on the gateway.

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

Each package has:

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

If you have R71.x with SSL VPN enabled, put the **TRAC.cab** file in a different directory, as shown in the instructions.

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

Unattended (ATM) Clients

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



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

To distribute the Remote Access Clients from the gateway:

1. On the gateway, in the `$FWDIR/conf/extender/CSHELL` directory, back up the `TRAC.cab` and `trac_ver.txt` files.
For R71.x, back up the `TRAC.cab` file in:
`$CVPNDIR/htdocs/SNX/CSHELL`
2. Download the Remote Access Clients E80.41 Automatic Upgrade file from the Endpoint Security Client E80.41 homepage (<http://supportcontent.checkpoint.com/solutions?id=sk91181>).
3. Put the new `TRAC.cab` and `ver.ini` files in the same directory on the gateway:
`$FWDIR/conf/extender/CSHELL`
For R71.x, put the `TRAC.cab` file also in:
`$CVPNDIR/htdocs/SNX/CSHELL`
4. On a non-Windows gateway, run: `chmod 750 TRAC.cab`

5. Edit the `trac_ver.txt` file in the directory and change the version number to the number in the new `ver.ini`.
6. Make sure the client upgrade mode is set:
 - a) Open the SmartDashboard.
 - b) Open **Policy > Global Properties > Remote Access > Endpoint Connect**.
 - c) Set the **Client upgrade mode** to **Ask user** (to let user confirm upgrade) or **Always upgrade** (automatic upgrade).
 - d) Click **OK**.
7. Install the policy.

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

 - If users had Endpoint Security VPN R75, it keeps the existing settings.
 - If users had Endpoint Connect R73, it automatically upgrades to Endpoint Security VPN.

Configuring Upgrades

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



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

To configure how to deploy changes to the client:

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

Endpoint Security VPN for Unattended Machines (ATMs)

SmartDashboard-managed Endpoint Security VPN can be installed and managed locally on unattended machines, such as ATMs. Unattended clients are managed with CLI ("[Remote Access Clients Command Line](#)" on page 125) and API and do not have a User interface. SmartEndpoint-managed Endpoint Security VPN, Check Point Mobile for Windows and SecuRemote do not have unattended versions.

See the Remote Access Clients API Reference Guide <http://supportcontent.checkpoint.com/solutions?id=sk91181> for API details.

There are different installation and upgrade files for unattended clients versus regular attended clients. They are called:

- Remote Access Clients (for Windows) MSI file for ATM
- Remote Access Clients (for Windows) Automatic Upgrade Package for ATM



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

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

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

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

Configuring the client for ATMs

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

- Make sure that there is an application that uses the client API to start and monitor the connection. You can configure the client for **always-connect** (rather than the API). But we do not recommend this if you use **secondary connect**. If the primary tunnel disconnects and the machine reboots, a client in **always-connect** will not connect to the backup tunnel. It will try to connect to the primary tunnel. If you want always-connect and secondary connect, we recommend that you use a 3rd party code to switch to the secondary tunnel on failover.
- Make sure the ATM machine has a certificate in the CAPI, and that the client is configured for **automatic CAPI re-authentication**.

Administrators can configure username and password caching for ATM devices in the Windows registry. Credentials are saved encrypted in the registry per site. This feature does not depend on password caching. See Remote Access Clients Command Line (on page 125) for feature usage.

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

To enable automatic CAPI re-authentication:

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

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

3. Save the file and install policy.
4. Apply this configuration to all gateways.



Note - To learn more about the TTM file, see The Configuration File (on page 103).

Configuring the Client Package

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

To configure the package for ATMs:

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

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



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

3. Go to `c:\program files\checkpoint\endpoint` and run `AdminMode.bat`.
4. Go to **VPN Options > Administration** tab.
5. In the **Input MSI Package path** field, enter the pathname of **CheckpointEndpointSecurityForATM.msi**.
6. Select **Replace user's configuration when upgrading**.
7. In **Select a product**, select **Endpoint Security VPN**.
8. Click **Generate**.
9. Save the MSI to the local disk.

10. Enable **No Office Mode** on the MSI:

- a) At the Windows command prompt, go to `c:\program files\checkpoint\endpoint`.
- b) Run this command:

```
cpmsi_tool.exe CheckPointEndpointSecurityForATM.msi -NO_OFFICE_MODE 1
```

Deploying the Client Package Manually

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

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

To upgrade the client manually:

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

Using DNS for Automatic Site Detection

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

This DNS query:

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

To configure automatic DNS site detection:

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

Property	Value
Service	CHECKPOINT_RA_
Protocol	_tcp
Port number	443
Host offering this service	Name of the 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 Step 2: **Replace the trac.config file on a client machine** ("[Using the Update Configuration Tool](#)" on page 44).

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

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

Usage for Update Configuration Tool

Syntax

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

Parameters

Parameter	Description
old <code>trac.config</code> file name and path	The path on the user's machine to the temporary location where they put the old <code>trac.config</code> 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 Remote Access Clients services from the CLI:

```
net stop tracsrvwrapper
```

2. Copy `trac.config` from the current installation directory (for example, `C:\Program Files\CheckPoint\Endpoint Connect\`) to a temporary directory (for example `C:\windows\temp`).
3. Copy the new `trac.config` file (created in Step 1) to the installation directory (for example, `C:\Program Files\CheckPoint\Endpoint Connect\`).
4. Run the `update_config tool` command to transfer user information from the old file to the new file. For example:

```
update_config_tool "C:\Windows\Temp\trac.config" "C:\Program Files\CheckPoint\Endpoint Connect\"
```
5. Start Remote Access Clients services from the CLI:

```
net start tracsrvwrapper
```

Chapter 3

Helping Your Users

In This Chapter

Simple Installation	46
Remote Access Clients Client Icon	46
Helping Users Create a Site	47
Helping Users with Basic Client Operations	50

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

Simple Installation

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

To install Remote Access Clients, users do this:

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



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

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

Remote Access Clients Client Icon

The client icon shows the status of the client.

SmartDashboard-managed:

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.

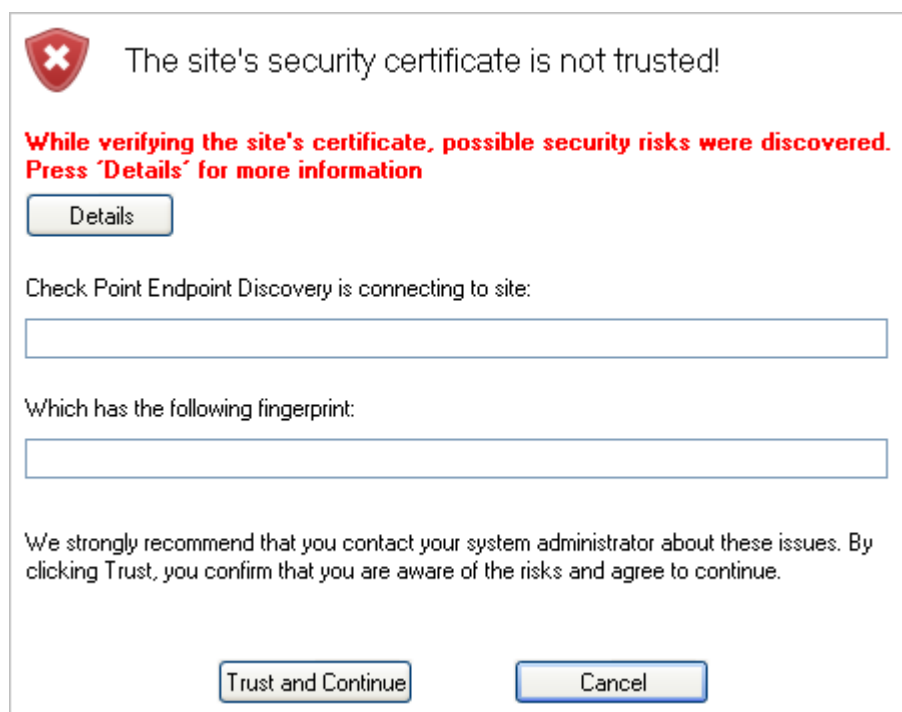
Helping Users Create a Site

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

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

Preparing the Gateway Fingerprint

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



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

To prepare the gateway fingerprint:

1. In SmartDashboard, click **Manage** menu > **Servers and OPSEC Applications**.
2. In the **Servers and OPSEC Applications** window, select the Certificate Authority and click **Edit**.
3. Open the **Local Security Management Server** or **OPSEC PKI** tab and click **View**.

If a DNS server is configured and the client is within the internal network, the client detects the VPN site automatically.

Server address or Name:	<input type="text" value="example.domain.com"/>
<input checked="" type="checkbox"/> Display name:	<input type="text" value="My Gateway"/>


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

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

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


- Compare the site fingerprint with the SIC fingerprint on the gateway.
- Click **Details** to see additional warnings.
- If site details are correct, click **Trust and Continue**. The fingerprint is stored in the Windows registry and the security warning is not opened again for the site, even if the client is upgraded.

The wizard displays the authentication method step.



Authentication Method

Select the authentication method to be used.



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

Certificate
Click if you use Hardware tokens or any other certificate type.

SecurID
Click if you use RSA SecurID.

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

Secure Authentication API (SAA)
Click if you use third party authentication.

- Give your users the authentication materials they need ("[Authentication Schemes and Certificates](#)" on page 26).
- The user selects the correct method and clicks **Next**.
 - If **Certificate**, the user selects **PKCS#12** or **CAPI** (make sure the user knows which to select), and clicks **Next**.
 - If **SecurID**, the user selects the type, and clicks **Next**.
 - If **Secure Authentication API (SAA)**, the user selects that and a new page opens to select the type of SAA and the DLL file. If a DLL file is already configured for the site, users do not have to select a file. Then click **Next**.
- The user clicks **Finish** and a message shows: Would you like to connect?
If the user clicks **Yes**, the client connects to the gateway and a VPN tunnel is created.

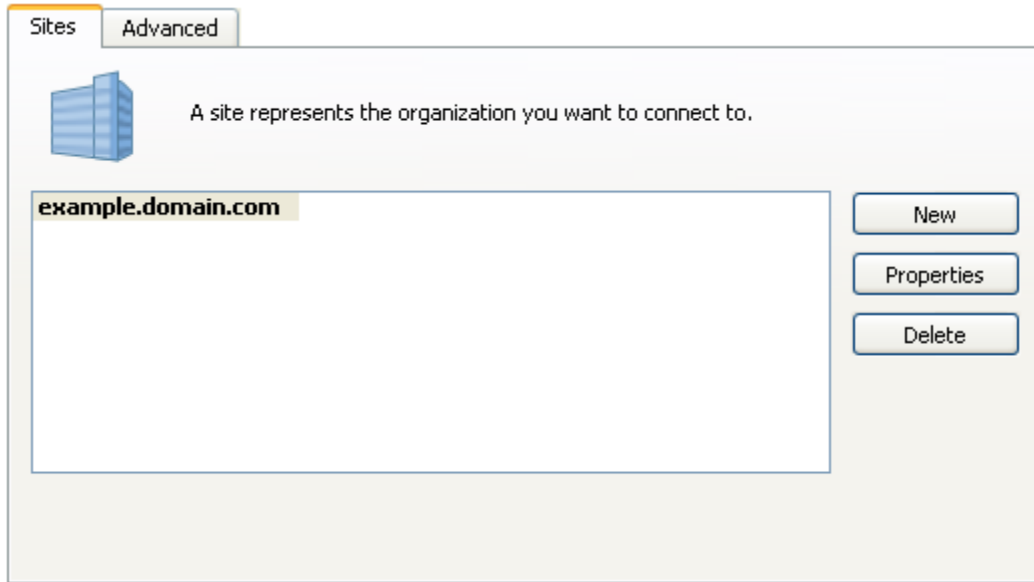
Opening the Site Wizard Again

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

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

- Right-click the client icon and select **VPN Options**.

The Options window opens.



2. On the **Sites** tab, click **New**.
The Site Wizard opens.
OR
3. Right-click the client icon and select **Connect to**.
4. In the **Site** drop-down, select **New Site**.
The Site Wizard opens.

Helping Users with Basic Client Operations

Users can do basic client operations from the client icon.



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 SmartDashboard-managed only.
Shutdown Client	Closes the Client - In SmartDashboard-managed only. An open VPN is closed. A background service continues to run and responds to CLI commands. To stop the service: <code>net stop tracsrvwrapper</code> If you close Endpoint Security VPN and stop the service, the desktop firewall still enforces the security policy.

For more VPN options in SmartEndpoint-managed clients:

1. Right -click the client icon and select **Display Overview**.
2. Click Remote Access VPN Blade.

3. Click one of the link for more options:

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

Chapter 4

Configuring Client Features

In This Chapter

Intel Smart Connect Technology	52
HotSpot Registration	52
Installing Desktop Security Policy	53
Managing Desktop Firewalls	53
Secure Domain Logon (SDL)	59
Multiple Entry Point (MEP)	61
Secondary Connect	66
Global Properties for Remote Access Clients Gateways	67
Split DNS	75
Configuring Log Uploads	76
Configuring Post Connect Scripts	76
Office Mode IP Address Lease Duration	77
No Office Mode - Secondary Tunnel Resilience	77

Intel Smart Connect Technology

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

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

To enable automatic Intel Smart Connect Technology:

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

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

3. Save the file and install policy.

HotSpot Registration

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

To configure any port for HotSpot registration:

1. Open **GuiDBedit** and connect to the **Security Management Server**.
2. On the **Tables** tab, open **Global Properties > properties > firewall_properties > registration > ports**.
3. Remove the pre-defined ports.
4. Add a new element that uses the string value: **<any_port>**.
5. Click **File > Save all**.
6. Connect to the server using SmartDashboard.

7. Open **Global Properties > Remote Access > Hot Spot/Hotel Registration**

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

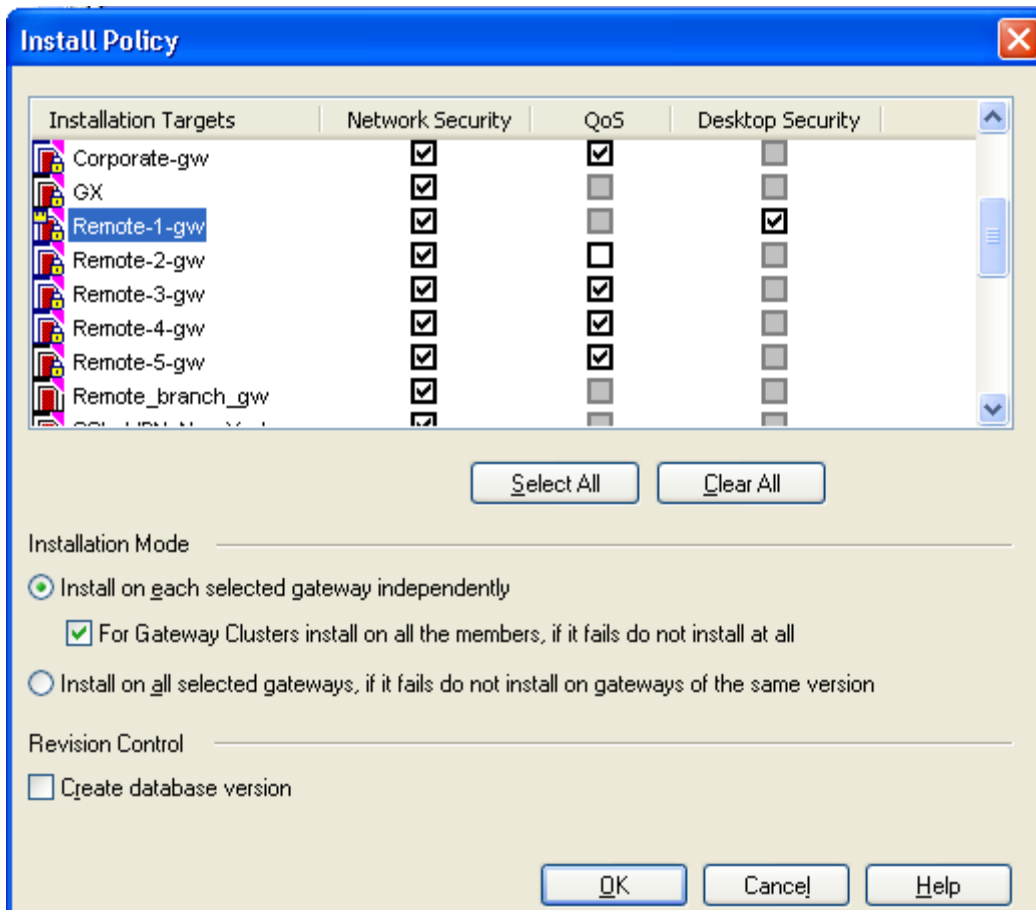


Note - The client must also be able to register to the Hotspot ("[hotspot_reg](#)" on page [130](#)).

Installing Desktop Security Policy

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

1. Click **Policy** menu > **Install**.
2. In the **Install Policy** window, select **Desktop Security** for the Endpoint Security VPN gateway. If this column is not available, you did not configure the Policy Server. This is necessary.

3. Click **OK**.

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

Managing Desktop Firewalls

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

In This Section

The Desktop Firewall	54
Rules	54
Default Policy	55
Location-Based Policies	55
Allow/Block IPv6 Traffic	56
Logs and Alerts	57
Wireless Hotspot/Hotel Registration	57
Planning Desktop Security Policy	57
Operations on the Rule Base	57
Making the Desktop Security Policy	57
Letting Users Disable the Firewall	59

The Desktop Firewall

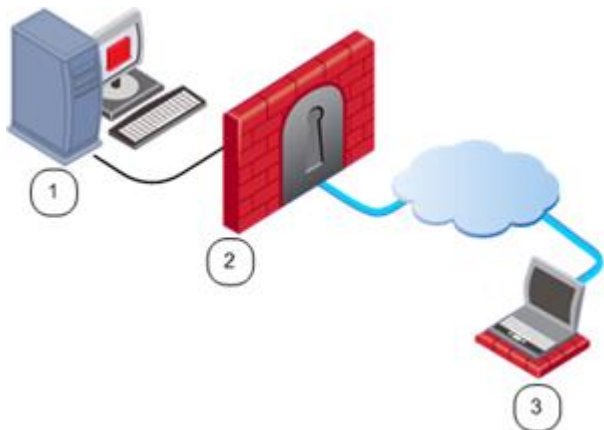
Endpoint Security VPN enforces a Desktop Security Policy on remote clients. You define the Desktop Security Policy in a Rule Base. Rules can be assigned to specific user groups, to customize a policy for different needs.



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

Endpoint Security VPN downloads the first policy from the gateway. It looks for and downloads new policies every time it connects or on re-authentication.

When Endpoint Security VPN makes a VPN connection, it connects to the gateway and downloads its policy. Endpoint Security VPN enforces the policy: accepts, encrypts, or drops connections, depending on their source, destination, and service.



Endpoint Security VPN Desktop Policy Architecture		
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 gateway and enforces policy on client computer

Rules

The Desktop Security Policy has Inbound and Outbound rules.

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

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

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

Implied Rules

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

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

User Granularity

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

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

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

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

Default Policy

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

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

Location-Based Policies

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

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

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



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

Location Awareness Policy Configuration

This release introduces two new properties in client configuration:

- `disconnected_in_house_fw_policy_enabled` – Defines if the feature is enabled or disabled.
Possible values are:
 - `true` – enabled
 - `false` – disabled (**default**)
- `disconnected_in_house_fw_policy_mode` – Defines which policy will be enforced after Location Awareness detection.
Possible values are:
 - `encrypt_to_allow` – Connected policy will be enforced, based on last connected user. Encrypt rules will be transformed to Allow rules (**default**).
 - `any_any_allow` – "Any – Any – Allow" will be enforced.

To enable Location Awareness for desktop firewall:

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

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

3. Save the file and install the policy.

To configure the location based policy:

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

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

3. Save the file and install the policy.



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

Allow/Block IPv6 Traffic

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

To allow IPv6 traffic to the client:

1. On the Security Gateway, open this file for editing:
`$FWDIR/conf/trac_client_1.ttm`
2. Add these lines:

```
: allow_ipv6 (
    :gateway (allow_ipv6
              :default (true)
            )
)
```

3. Close and 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 SmartView Tracker.

Wireless Hotspot/Hotel Registration

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

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

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

A proxy ("[Pre-Configuring Proxy Settings](#)" on page 33) might be required.

Planning Desktop Security Policy

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

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

Operations on the Rule Base

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

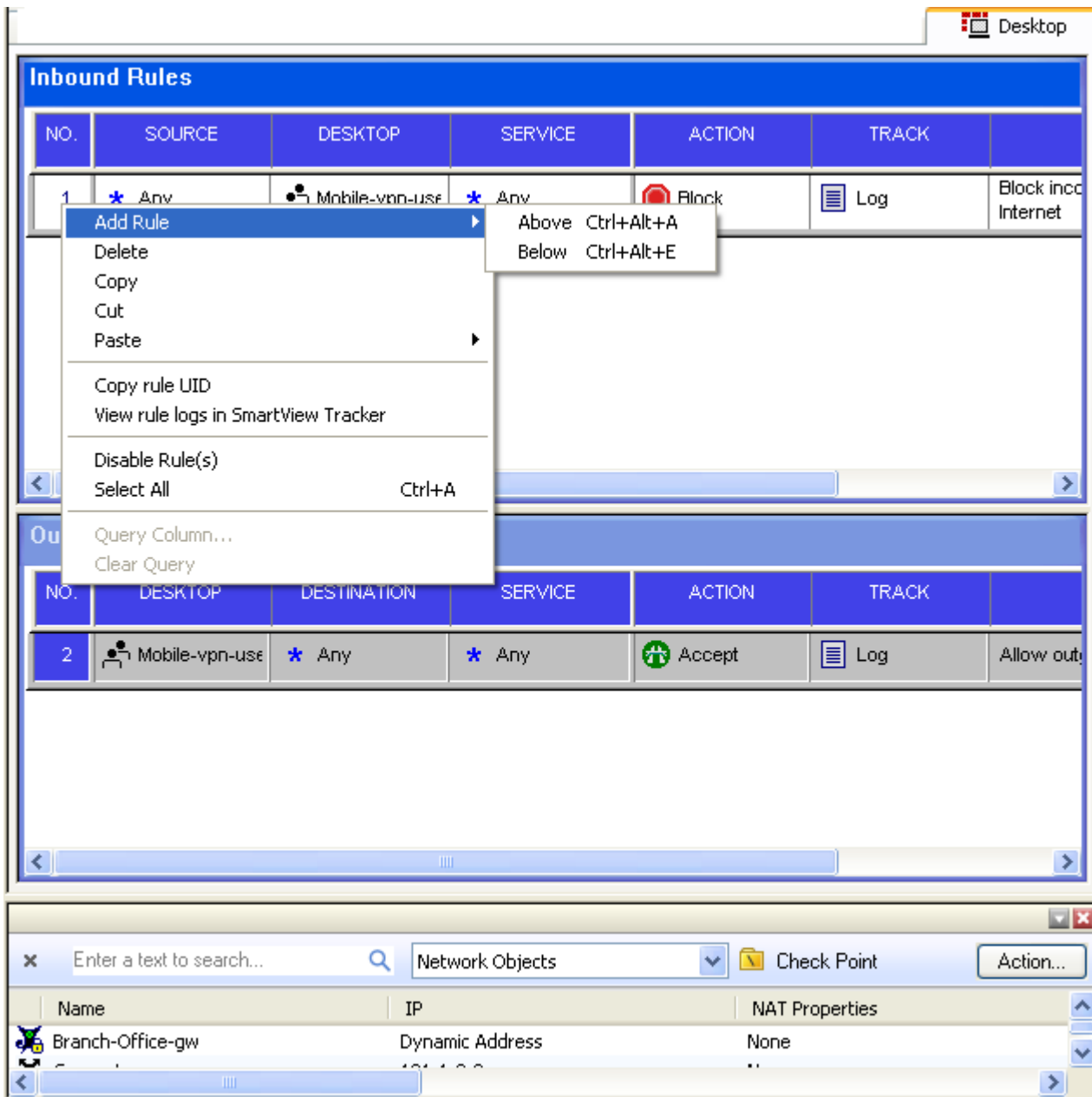
- **Add** - Add a rule above or below the selected rule.
- **Disable** - Rules that are currently not implemented, but may be in the future, can be disabled.
- **Delete** - Delete rules which are no longer necessary.
- **Hide** - Hide rules that are irrelevant to your current view, to enhance readability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

Making the Desktop Security Policy

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

To make a Desktop Security Policy:

1. Open the **Desktop** tab.



2. Configure the rules. For each rule, you can specify users for whom the rule is applied.
 In inbound rules, **Desktop** (Endpoint Security VPN) is the destination.
 In outbound rules, **Desktop** is the source.
3. Install the policy (**Policy** menu > **Install**).
 Install the Desktop security policy on the gateways that are configured to handle Endpoint Security VPN traffic.

SecureClient and Endpoint Security VPN

If you have SecureClient and Endpoint Security VPN installed on the same machine, see *Troubleshooting Dual Support* in one of the E75.20 Upgrade Guides (<http://supportcontent.checkpoint.com/solutions?id=sk65209>).

Making a Rule for FTP

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

To add the Active FTP Rule:

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

Letting Users Disable the Firewall

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

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

To change the Allow disable firewall setting:

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

Secure Domain Logon (SDL)

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

In this section

Configuring SDL	59
Configuring Windows Cached Credentials	60
Using SDL in Windows XP	60
SDL in Windows Vista and Windows 7	60
Disable or Enable SDL on Internal Network	61

Configuring SDL

To enable SDL:

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

SDL for SmartDashboard-Managed Clients**To create an SDL-enabled client:**

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

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



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

To help users enable SDL on a client:

1. Right-click the client icon and select **VPN Options**.
2. In **Options > Advanced**, select **Enable Secure Domain Logon (SDL)**.

3. Click **OK**.
4. Restart the computer and log in.

To enable Remote Access Clients to use SDL:

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

Configuring Windows Cached Credentials

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

To configure this option in the client registry:

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

Using SDL in Windows XP

To use SDL in Windows XP:

1. When the Windows Logon window is open, the user enters the operating system credentials and clicks **OK**.
The Remote Access Clients **Logon** window opens.
2. The user enters the Remote Access Clients credentials.

If logon fails and no cached information is used, wait one minute and try again.

You can customize the Remote Access Clients installation packages with SDL enabled by default.

SDL in Windows Vista and Windows 7

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

- Explicit
- Implicit

Using Explicit Mode

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

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

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



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.



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

Disable or Enable SDL on Internal Network

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

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

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

Value	Meaning
true (default)	The SDL window does not show when the client is inside the LAN or VPN domain.
false	The SDL window always shows.

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

Multiple Entry Point (MEP)

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

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



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

Remote Access Clients automatically detects and uses MEP topology.

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

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

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

Configuring Entry Point Choice

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

- **First to Respond** - The first gateway to reply is chosen and the VPN tunnel is between that gateway and the client. The client asks for a response for each connection.

Recommendation: If you have multiple gateways that are geographically distant. For example, an organization has three gateways: London, Sundsvall, and Paris. Usually, the London gateway responds first to clients in England and is their entry point to the internal network. If the London gateway goes down, these users access the network through the Paris or Sundsvall gateway that responds first.

- **Primary-Backup** - One or multiple auxiliary gateways give high availability for a primary gateway. Clients are configured to connect with the primary gateway, but change to a Backup gateway if the Primary goes down.

Recommendation: If you have multiple gateways, and one is stronger or connects faster, set the stronger machine as the primary. Clients use the backup if the primary is unavailable.

- **Load Distribution** - Clients randomly select a gateway.
Recommendation: If you have multiple gateways of equal performance. The traffic of the clients is shared between the gateways. Each client creates a tunnel with a random, available gateway.
- **Geo-Cluster DNS Name Resolution** - You can enable Geo-Clustering instead of MEP, however we recommend MEP as it is easier to manage and gives better performance. Geo-Cluster resolves gateway DNS names based on location.

Defining MEP Method

MEP configuration can be implicit or manual.

- **Implicit** - MEP methods and gateway identities are taken from the topology and configuration of gateways that are in fully overlapping encryption domains or that have Primary-Backup gateways.
- **Manual** - You can edit the list of MEP Security Gateways in the Remote Access Clients TTM file.

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

To define MEP topology:

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

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

3. Set the value of `:default` to:
 - `true` - For implicit configuration
 - `false` - For manual configuration
4. **For Manual MEP only:** Make sure that `enable_gw_resolving` is `true`
5. Save the file.
6. Install the policy.

Implicit MEP

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

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

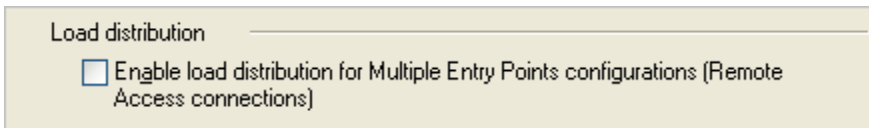
```
automatic_mep_topology (true)
```

Configuring Implicit First to Respond

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

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

- NGX R65 and R70: VPN Basic
- R71 and higher: VPN Advanced



To configure First to Respond MEP:

1. Find out which gateways are in the VPN domain. In the VPN CLI, run:
`vpn overlap_enddom`
2. Create a host group and assign all of these gateways to it.
3. In the **Properties** window of each gateway network object > **Topology** page > **VPN Domain** section, select **Manually defined** and then select the host group of MEP gateways.
4. Click **OK**.
5. Install the policy.

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

Configure the same grace period on each gateway.

To give preference to the selected gateway:

1. On each gateway, open the `$FWDIR/conf/trac_client_1.ttm` configuration file.
2. Find the `mep_prefer_chosen_gw_grace_period` parameter.
3. Set the grace period in milliseconds.
4. Save the file.
5. Install the policy.

Configuring Implicit Load Distribution

To configure implicit MEP for random gateway selection:

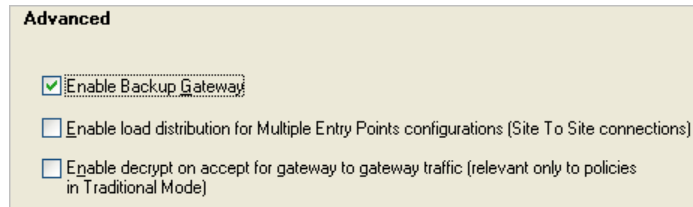
1. Open **Global Properties**.
2. Open **IPSec VPN > Advanced** (or **VPN > Advanced**).
3. Select **Enable load distribution for Multiple Entry Point configurations (Site to Site connections)**.
4. Define the same VPN domain for all the gateways:
 - a) Create a group of the gateways.
 - b) On the **Properties**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

Configuring Implicit Primary-Backup

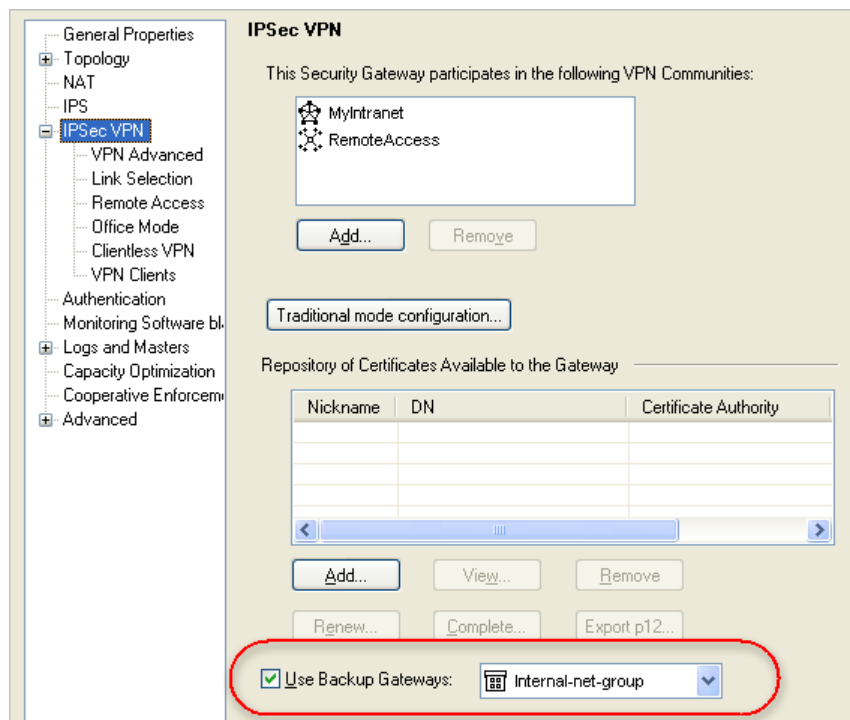
Configure the VPN Domain that includes the Primary gateway and another domain that includes only the backup gateway. Configure each gateway as either the Primary gateway or a backup gateway.

To configure the primary gateway:

1. Open **Global Properties** window > **VPN > Advanced**, select **Enable Backup Gateway**.



2. In the network objects tree, **Groups** section, create a group of gateways to act as backup gateways.
3. Open the VPN properties of the Primary gateway:
 - NGX R65 and R70: Gateway properties > **VPN**
 - R71 and higher: Gateway properties > **IPSec VPN**
4. Select **Use Backup Gateways**, and select the group of backup gateways.



This gateway is the primary gateway for this VPN domain.

5. For each backup gateway, make a VPN domain that does not include IP addresses that are in the Primary VPN domain or the other backup domains.
If the backup gateway already has a VPN domain, you must make sure that its IP addresses do not overlap with the other VPN domains.
 - a) Create a group of IP addresses not in the other domains, or a group that consists of only the backup gateway.
 - b) On the **Properties** window of the backup network object > **Topology > VPN Domain** section, select **Manually defined**.
 - c) Select the group.
6. Click **OK**.
7. Install the policy.

Manual MEP

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

To configure the gateways for MEP:

1. On a gateway, open `$FWDIR/conf/trac_client_1.ttm`.
2. Search for the `enable_gw_resolving` attribute:

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

3. Make sure the attribute is set to its default value: **true**.
4. Search for the `automatic_mep_topology` attribute, and make sure its value is **false**.
5. Manually add the `mep_mode` attribute:

```
:mep_mode (
    :gateway (
        :default (xxx)
    )
)
```

Where xxx is a valid value:

- **first_to_respond**
 - **primary_backup**
 - **load_sharing**
 - **dns_based** - Use this to configure Geo-Clusters ("[Configuring Geo-Cluster DNS Name Resolution](#)" on page 65).
6. Manually add the `ips_of_gws_in_mep` attribute:

```
:ips_of_gws_in_mep (
    :gateway (
        :default (192.168.53.220&#192.168.53.133&#)
    )
)
```

These are the IP addresses the client should try.

- IP addresses are separated by an ampersand and hash symbol (&#).
 - The last IP address in the list has a final &#.
7. Save the file.
 8. Install the policy.

Making a Desktop Rule for MEP

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

To add the MEP Rule:

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

Configuring Geo-Cluster DNS Name Resolution

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

To enable Geo-Cluster DNS Name Resolution:

1. On the Security Gateway, open `$FWDIR/conf/trac_client_1.ttm`.
2. Change the `:default` attribute, located in the `:enable_gw_resolving` attribute, to **true**.

```

:enable_gw_resolving (
  :Security Gateway (
    :map (
      :false (false)
      :true (true)
      :client_decide (client_decide)
    )
    :default (true)
  )
)

```

3. Manually add the `mep_mode` attribute and set it to `dns_based`.
4. Make sure that the `automatic_mep_topology` is `false`.
5. Save the file.
6. Install the policy.

To disable Geo-Cluster DNS Name Resolution (and enabling DNS IP address cache):

1. On the Security Gateway, open `$FWDIR/conf/trac_client_1.ttm`.
2. Do one of these:
 - Set the `automatic_mep_topology` to `true`
 - Set the `mep_mode` attribute to one of the options that is not "dns_based." See Manual MEP (on page 64).
 - Disable the MEP entirely by setting the `enable_gw_resolving` attribute to `false`.
3. Save the file.
4. Install the policy.

Secondary Connect

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

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

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

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

Secondary Connect is compatible with legacy SecureClient settings.

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

Configuring Secondary Connect

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

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

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

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

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

To configure Secondary Connect on each gateway:

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

```

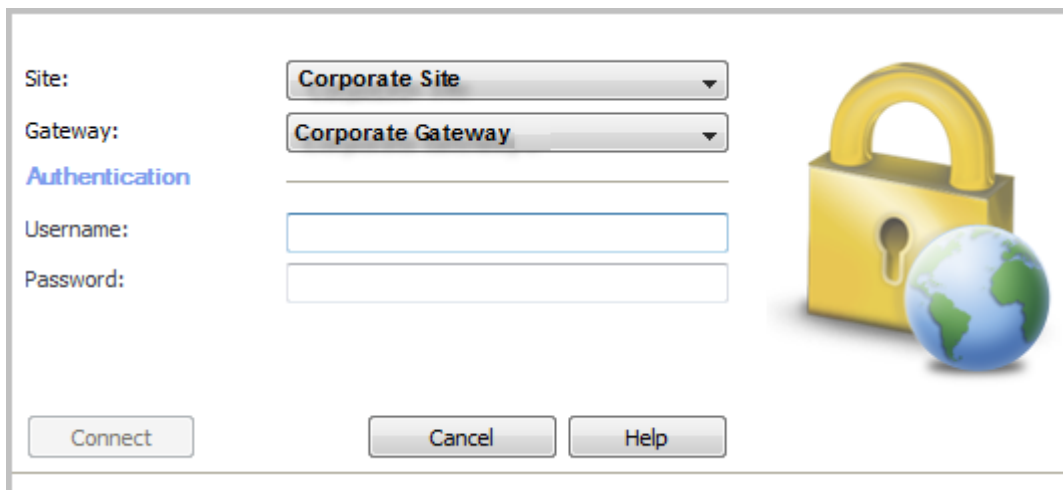
:enable_secondary_connect (
    :gateway (
        :map (
            :true (true)
            :false (false)
            :client_decide (client_decide)
        )
        :default (true)
    )
)

```

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

Secondary Connect for Users

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



The screenshot shows a VPN client authentication window. On the left, there are two dropdown menus: 'Site' with 'Corporate Site' selected and 'Gateway' with 'Corporate Gateway' selected. Below these is a section titled 'Authentication' with two input fields for 'Username' and 'Password'. At the bottom are three buttons: 'Connect', 'Cancel', and 'Help'. On the right side of the window is a graphic of a yellow padlock and a globe.

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

Global Properties for Remote Access Clients Gateways

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

To configure Remote Access Clients features in Global Properties:

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

3. Open **Remote Access > Endpoint Connect**.


Endpoint Connect

Authentication Settings

Enable password caching: No

Cache password for: 1440 minutes

Re-authenticate user every: 480 minutes

Connectivity Settings  [Wide Impact](#)

Connect mode: Configured on endpoint client

Location Aware Connectivity: Configured on endpoint client [Configure...](#)

Disconnect when connectivity to network is lost: Configured on endpoint client

Disconnect when device is idle: Configured on endpoint client


Security Settings

Route all traffic to gateway: No

Configuration and Version Settings

Client upgrade mode: Ask user

Security Policy

Scan endpoint for spyware and compliance [Configure...](#)  [Wide Impact](#)

4. Set **Authentication Settings** (on page 68).
5. Set **Connectivity Settings**.
 - **Connect Mode** (on page 69)
 - **Location Aware Connectivity** (on page 69)
 - **Disconnect when connectivity to network is lost** ("Roaming" on page 69)
 - **Disconnect when device is idle** ("Idle VPN Tunnel" on page 72)
6. Set **Security Settings**.
7. Set **Client upgrade mode** ("Configuring Upgrades" on page 41).
8. Click **OK**.
9. Install the policy.

Authentication Settings

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

To configure authentication settings:

- **Enable password caching**
 - **No** (default) requires users to enter a password whenever they connect.
 - **Yes** retains the user password in a cache for a specified period.
- **Cache password for** - Password retention period in minutes (default = 1440), if password caching is enabled.



Note - For security reasons, the cache is cleared when the user explicitly disconnects, even if the cache period has not ended.

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

- **Re-authenticate** - Authentication timeout in minutes (default = 480), after which users must re-authenticate the current connection.
- **Caching and OneCheck User Settings** - In SmartEndpoint-managed clients, if you have OneCheck User Settings enabled, see the OneCheck User Settings settings in the *Endpoint Security Administration Guide*.

Connect Mode

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

- **Manual** - VPN connections are not initiated automatically. Users select a site and authenticate every time they need to connect.
- **Always connected** - Remote Access Clients will automatically establish a connection to the last connected gateway.
- **Configured on endpoint client** - Connection method is set by each Remote Access Clients client. In the client, this is configured on **Sites > Properties > Settings**.

Roaming

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

Disconnect when connectivity to network is lost:

- **No** - Roaming is set with unlimited timeout. The client keeps trying to reconnect until the session times-out.
- **Configured on the endpoint client** - Default client configuration sets this option to false, so roaming is unlimited by default. If you create a client MSI that enabled the Disconnect option for clients, roaming is limited to the set time-out (default is 2 minutes).
- **Yes** - Roaming is limited by a time-out that is 2 minutes by default. The client will give up on Roaming after the time-out passes and will fail the connection. If the time-out is set to 0, the client does not try to reconnect automatically after the main IP address changes.

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

To configure the roaming timeout:

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



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

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

Location Aware Connectivity

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

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

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

Choose a location awareness configuration.

- **Interface-topology-based** (recommended)

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

The Interface-topology-based setting was introduced in Check Point NGX R65 HFA 60 and is the preferred method. It is reliable and requires no special configuration, but it has no GUI (it uses GuiDBedit). If you have Check Point NGX R65 HFA 60, this setting requires the NGX R66 plug-in for Connectra on the management server.

- **Specific network considered as internal**

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

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

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

Enabling Location Awareness

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

To enable location awareness:

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

Configuring Location Awareness in pre-R75 Gateways

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

To configure location awareness for topology in gateways before R75:

1. After enabling the Location Awareness feature, save the policy and close SmartDashboard.
2. Connect to the Security Management Server with GuiDBedit.
3. On the **Tables** tab, open **Global Properties > Properties > firewall_properties**.
4. Open **endpoint_vpn_preferences > endpoint_vpn_la_preferences** and find the **la_use_gw_topology_to_identify_location** property.
5. Set the **Value** field in the **Edit** textbox to **True**.
6. Save and close.
7. Open SmartDashboard.
8. Install the policy.

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

1. In **Global Properties > Endpoint Connect**, click **Configure** by **Location Aware Connectivity**. The **Location Awareness Settings** window opens.
2. Select how clients are identified as internal.
 - a) **Client can access its defined domain controller.** Checks if the client can access the Microsoft Domain controllers on the internal network, which are inaccessible through a VPN tunnel.
 - b) **Client connection arrives from the following networks.** Define a group of known internal networks. Click **Manage** to define a network.



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

3. Click **OK**.
4. Install the policy.

Configuring Location Awareness in R75 and Higher Gateways

To configure Location Awareness in R75 and higher gateways:

1. In SmartDashboard, open **Global Properties > Remote Access > Endpoint Connect**.
2. In **Connectivity Settings**, in **Network Location Awareness**, select **Yes** and click **Configure**.
The **Network Location Awareness** window opens.
3. Select a location awareness configuration.
 - **The client connects to the gateway through one of its internal interfaces** - This option, based on interface topology, is recommended and selected by default.
 - **The client connects from this network or group**- Select this to specify the network considered to be internal.
 - **The client runs on a computer that can access its Active Directory Domain** - Bases the location on the availability of the Active Directory Domain Controller.
4. Click **OK**.

Optimizing External Network Detection

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

Location Awareness - Fast Detection of External Locations

Use these options to identify external sites,
and thereby enhance the performance of location awareness

Fast Detection of external locations _____

Regard wireless networks as external

Except for the following network names (SSIDs)

Wireless Network Names

New... Edit... Delete

Consider DNS suffixes which do not appear in the following list as external

DNS Suffix

New... Edit... Delete

Client Side Caching _____

Remember previously detected external networks

OK Cancel Help

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

- **Regard wireless networks as external.** Wireless networks you define here are internal. Of the client's wireless IP address is from one of these networks, it is considered internal. All other wireless networks are considered external.
- **Consider DNS suffixes which do not appear in the following list as external.** Define DNS suffixes that Remote Access Clients identifies as internal. If you select this option, make sure to define *all* internal DNS suffixes.
- **Remember previously detected external networks.** Networks previously identified by the client as external can be cached (on the client side), so future encounters with them result in immediate detection.

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

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

Configuring Location Awareness for NGX R65 Gateways

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

To configure location awareness in the configuration file:

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

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

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

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

Idle VPN Tunnel

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

To configure tunnel idleness:

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

Intelligent Auto-Detect

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

Current transports in use:

- **Visitor Mode** - TCP encapsulation over port 443 (by default). This mode is used when NAT-T is not available in routing to the gateway (for example, if there is a proxy or hotspot). Clients need Visitor Mode to operate.
- **NAT-T** - UDP encapsulation over port 4500 (by default) and preferable transport for IPsec. The IPsec protocol does not deal with NAT devices, so Remote Access Clients uses NAT-T encapsulation. NAT-T packets must go back to the client through the same interface they entered from. We recommend that you put the gateway in a public DMZ with one interface for all traffic. You can also deploy the default route as the outbound route to the Internet.

To configure auto-detect of network transports:

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

Smart Card Removal Detection

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

```
VPN tunnel has disconnected. Smart card was removed.
```

To enable Smart Card removal detection:

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

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

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

4. Save the file and install the policy.

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

Configuring Hotspot Access

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

To enable hotspot registration from SmartDashboard:

1. Open **Policy > Global Properties > Remote Access > Hot Spot/Hotel Registration**.

2. Select **Enable registration**.
3. Set the **Maximum** time and add **Ports** to be used.
4. Select a **Track** option.

The **Local subnets access** and **Allow access** options are not supported in Remote Access Clients.

5. Click **OK**.
6. Save and install the policy.



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

Configuring Automatic Hotspot Detection

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

To enable hotspot registration from the configuration file:

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

```

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

2. Change these parameters:

Parameter	Default	Description
hotspot_detection_enabled	true	Set to True to enable hotspot detection.
hotspot_registration_enabled	false	Set to True to enable a user to get a hotspot registration page (in embedded browser).

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

Split DNS

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

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

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

You can configure multiple SecuRemote DNS servers for different domains.

Configuring Split DNS

To configure a SecuRemote DNS server for Split DNS:

1. In SmartDashboard, go to the **Servers and OPSEC Applications** tab of the Objects Tree.
2. Right-click **Servers** and select **New SecuRemote DNS**.
The **SecuRemote DNS Properties** window opens.
3. In the **General** tab, enter a name for the server and select the host on which it runs.
4. In the **Domains** tab, click **Add** to add the domains that will be resolved by the server.
The Domain window opens,
5. Enter the **Domain Suffix** for the domain that the SecuRemote DNS server will resolve, for example, checkpoint.com.
6. In the **Domain Match Case** section, select the maximum number of labels that can be in the URL before the suffix. URLs with more labels than the maximum will not be sent to that DNS.
 - **Match only *.suffix** - Only requests with 1 label are sent to the SecuRemote DNS. For example, "www.checkpoint.com" and "whatever.checkpoint.com" but not "www.internal.checkpoint.com."
 - **Match up to x labels preceding the suffix**- Select the maximum number of labels. For example, if you select 3, then the SecuRemote DNS Server will be used to resolve "www.checkpoint.com" and "www.internal.checkpoint.com" but not "www.internal.inside.checkpoint.com".
7. Click OK two times to complete the configuration.
8. Install the policy.

Enabling or Disabling Split DNS

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

To change the setting for Split DNS on the gateway:

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

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

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

Configuring Log Uploads

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

To configure log uploads for Desktop Policy and SCV logs:

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

Configuring Post Connect Scripts

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

To set the script path:

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

Office Mode IP Address Lease Duration

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

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

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

No Office Mode - Secondary Tunnel Resilience

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

New features:

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



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

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

Secondary Tunnel Resilience

Terminology:

- **Primary Gateway**
The gateway responsible for client configuration.
- **Secondary Gateway**
The second gateway in a tunnel.
- **Default Gateway:**
The gateway chosen as first to connect.
- **Roaming**
A feature that detects tunnel disconnection status and tries to reconnect it.

How Secondary Tunnel Resilience Works

Connection State	If Tunnel is Disconnected From:	Roaming Tries to:
Tunnel to Primary Gateway (A) is connected	Primary Gateway (A)	Reconnect the tunnel.

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

Chapter 5

Secure Configuration Verification (SCV)

In This Chapter

Check Point SCV Checks	79
Configuring the SCV Policy	80
Configuring SCV Enforcement	80
Configuring SCV Exceptions	81
Traditional Mode	81
Installing and Running SCV Plugins on the Client	81
SCV Policy Syntax	82
Deploying a Third Party SCV Check	102

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

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



Note - SCV is not supported in SecuRemote.

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

Check Point SCV Checks

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

- **OS Monitor** - Verifies Operating System version, Service Pack, and Screen Saver configuration (activation time, password protection, *etc.*).
- **HotFix Monitor** - Verifies that operating system security patches are installed, or not installed.
- **Group Monitor** - Verifies that the user logged into the operating system and is a member of specified Domain User Groups.
- **Process Monitor** - Verifies that a process is running, or not running, on the client machine (for example, that a file sharing application is not running, or that Anti-Virus is running).
- **Browser Monitor** - Verifies Internet Explorer version and configuration settings, such as Java and ActiveX options.
- **Registry Monitor** - Verifies System Registry keys, values, and their contents.
- **Anti-Virus Monitor** - Verifies that an Anti-Virus is running and checks its version. Supported: Norton, Trend Office Scan, and McAfee.
- **SCV Monitor** - Verifies the version of the SCV product, specifically the versions of the SCV DLLs installed on the client's machine.

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

Configuring the SCV Policy

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



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

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

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



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

Configuring SCV Enforcement

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

To configure SCV Enforcement for the Gateways:

1. In SmartDashboard, select **Policy > Global Properties**.
2. Open **Remote Access > Secure Configuration Verification (SCV)**.
3. Select **Apply Secure Configurations on Simplified Mode**.

This causes the gateway to verify client compliance.



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

4. In the **Upon Verification failure area**, set the action of the gateway if a client fails one or more SCV checks and is non-compliant.
 - **Block client's connection**
 - **Accept and log client's connection**

If you block non-compliant clients, you can set up exceptions to allow the clients to download remediations.

5. Make sure that there is at least one rule in the firewall Rule Base that has the **RemoteAccess** VPN community object in the **VPN** column.
6. Click **OK**.
7. Install the policy.



Note - There are additional sections in the **Secure Configuration Verification (SCV)** page in SmartDashboard:

- **Basic configuration verification on client's machine**
- **Configuration Violation Notification on client's machine**

These settings are not supported for Remote Access Clients.

Configuring SCV Exceptions

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

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

To make exceptions for non-compliant remote clients:

1. Select the **Apply Secure Configuration Verification on Simplified mode Firewall Policies** option. The **Exceptions** button activates.
2. Click **Exceptions**.
The Secure Configuration Verification Exceptions window opens.
3. Click **Add**.
4. Double-click **None** and select a host and service.
5. Click **OK**.

Traditional Mode

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

To configure SCV enforcement in Traditional mode:

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

Installing and Running SCV Plugins on the Client

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

When the Remote Access Clients connect to the gateway:

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

SCV Policy Syntax

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

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

Sets and Sub-sets

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

Sample Syntax:

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

Expressions

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

Example:

```
:browser_major_version (7)
```

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

Grouping Expressions

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

Example:

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

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

Influential Expressions

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

Example:

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

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

Logical Sections

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

begin_or

begin_or (or#) - end (or#)

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

Example:

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

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

begin_and

begin_and (and#) - end (and#)

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

Example:

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

```

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

```

The first AND section checks if the version of IE \geq 7.0. The second AND section checks whether the version of IE is \leq 6.0. The entire section is **true** if the version is greater than (or equal to) 7.0, OR lower than (or equal to) 6.0.

Expressions and Labels with Special Meanings

Some expressions and labels are reserved for specific purposes.

Example:

```

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

```

begin_admin

`begin_admin (admin) - end (admin)`

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

mismatchmessage

`mismatchmessage ("Message")`

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

send_log

send_log (alert)

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

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

The local.scv Sets

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

SCVNames

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

Sample:

<pre> : (SCVCheckName1 :type (plugin) :parameters (:Expression1 (value) :Expression2 (value) :begin_admin (admin) :send_log (alert) :mismatchmessage ("Failure Message") :end (admin))) </pre>	<p>name of the check</p> <p>check is done by an SCV DLL plugin</p> <p>subset for rules and actions</p>
---	--

SCVEpsNames

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

SCVPolicy

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

Sample:

<pre> :SCVPolicy (: (SCVCheckName1) : (SCVCheckName2)) </pre>



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

SCVEpsPolicy

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

SCVGlobalParams

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

SCV Parameters

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

Anti-Virus monitor

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

Parameter	Description
Type ("av_type")	Type of Anti-Virus. For example, "Norton", "VirusScan", "McAfee", "OfficeScan", or "ZoneLabs".
Signature (x)	Required Virus definition file signature. The signature's format depends on the Anti-Virus type. <ul style="list-style-type: none"> Norton Antivirus example: ">=20031020" (format for Norton's AV signature is "yyyymmdd") TrendMicro Officescan example: "<650" McAfee VirusScan example: (">404291") for a signature greater than 4.0.4291 Zone Labs format: (">X.Y.Z") where X = Major Version, Y = Minor Version, and Z = Build Number of the .dat signature file

BrowserMonitor

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

- `restricted_download_signed_activex`
- `restricted_run_activex`
- `restricted_download_files`
- `restricted_java_permissions`

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

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

Parameter	Description
<code>browser_major_version</code> (#)	Major version number of Internet Explorer. If this field does not exist in the local.scv file, or if this value is 0, the IE version will not be checked as part of the BrowserMonitor check.

Parameter	Description
<code>browser_minor_version (#)</code>	Internet Explorer minor version number.
<code>browser_version_operand (">=")</code>	The operator used for checking the Internet Explorer's version number.
<code>browser_version_mismatchmessage ("Please upgrade your Internet Browser.")</code>	Message to be displayed for a non-verified configuration of Internet Explorer.
<code>intranet_download_signed_activex (enable)</code>	The maximum permission level that IE should have for downloading signed ActiveX controls from within the local Intranet.
<code>intranet_run_activex (enable)</code>	The maximum permission level that IE should have for running signed ActiveX controls from within the local Intranet.
<code>intranet_download_files (enable)</code>	The maximum permission level that IE should have for downloading files from within the local Intranet.
<code>intranet_java_permissions (low)</code>	The maximum security level that IE Explorer should have for running java applets from within the local Intranet.
<code>trusted_download_signed_activex (enable)</code>	The maximum permission level that IE should have for downloading signed ActiveX controls from trusted zones.
<code>trusted_run_activex (enable)</code>	The maximum permission level that IE should have for running signed ActiveX controls from trusted zones.
<code>trusted_download_files (enable)</code>	The maximum permission level that IE should have for downloading files from trusted zones.
<code>trusted_java_permissions (medium)</code>	The maximum security level that IE should have for running java applets from trusted zones.
<code>internet_download_signed_activex (disable)</code>	The maximum permission level that IE should have for downloading signed ActiveX controls from the Internet.
<code>Internet_run_activex (disable)</code>	The maximum permission level that IE should have for running signed ActiveX controls from the Internet.
<code>internet_download_files (disable)</code>	The maximum permission level that IE should have for downloading files from the Internet.
<code>internet_java_permissions (disable)</code>	The maximum security level that IE should have for running java applets from the Internet.
<code>restricted_download_signed_activex (disable)</code>	The maximum permission level that IE should have for downloading signed ActiveX controls from restricted zones.
<code>restricted_run_activex (disable)</code>	The maximum permission level that IE should have for running signed ActiveX controls from restricted zones.
<code>restricted_download_files (disable)</code>	The maximum permission level that IE should have for downloading files from restricted zones.
<code>restricted_java_permissions (disable)</code>	The maximum security level that IE should have for running java applets from restricted zones.

Parameter	Description
send_log (type)	Whether to send a log to Security Management server for specifying that the client is not verified: log or alert . Does not support begin_admin .
internet_options_mismatch_message ("Your Internet browser settings do not meet policy requirements")	Mismatch message for the Internet Explorer settings.

Groupmonitor

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

Parameter	Description
"builtin\administrator" (false)	A name of a user group. The user must belong to this group for the machine configuration to be verified.

HotFixMonitor

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

Parameter	Description
HotFix_Number (true)	A number of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: "823980(true)" verifies that Microsoft's RPC patch is installed on the operating system.
HotFix_Name (true)	The full name of a system HotFix to be checked. In order for the machine to be verified, the HotFix should be installed, for example: "KB823980(true)" verifies that Microsoft's RPC patch is installed on the operating system.

HWMonitor

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

Parameter	Description
cputype ("GenuineIntel")	The CPU type as described in the vendor ID string. The string has to be exactly 12 characters long. For example: "GenuineIntel", or "AuthenticAMD", or "aaa bbb ccc " where spaces count as a character.
cpufamily(6)	The CPU family.
cpumodel(9)	The CPU model.

OsMonitor

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

- major_os_version_number_xp
- minor_os_version_number_xp
- os_version_operand_xp
- service_pack_major_version_number_xp

- `service_pack_minor_version_number_xp`
- `service_pack_version_operand_xp`

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

OSMonitor does not support `begin_or` or `begin_and`.

Parameter	Description
<code>enforce_screen_saver_minutes_to_activate (3)</code>	Time in minutes for the screen saver to activate. If the screen saver does not activate within this time period, then the client is not considered verified. In addition, the screen saver must be password protected.
<code>screen_saver_mismatchmessage (“Your screen saver settings do not meet policy requirements”)</code>	Mismatch message for the screen saver check. The screen saver will not be checked if the property “ <code>enforce_screen_saver_minutes_to_activate</code> ” does not appear, or if the time is set to zero.
<code>major_os_version_number_xp (5)</code>	Specifies the major version required for Windows XP operating systems to be verified.
<code>minor_os_version_number_xp (1)</code>	Specifies the minor version required for Windows XP operating systems to be verified.
<code>os_version_operand_xp (“>=”)</code>	Operator for checking the operating system’s service pack on Windows XP
<code>service_pack_major_version_number_xp (0)</code>	Specifies the major service pack version required for Windows XP operating systems to be verified.
<code>service_pack_minor_version_number_xp (0)</code>	Specifies the minor service pack version required for Windows XP operating systems to be verified.
<code>service_pack_version_operand_xp (“>=”)</code>	Operator for checking the operating system’s service pack on Windows XP.
<code>major_os_version_number_8 (6)</code>	Specifies the major version required for Windows 8 operating systems to be verified.
<code>minor_os_version_number_8 (2)</code>	Specifies the minor version required for Windows 8 operating systems to be verified.
<code>os_version_operand_8 (“==”)</code>	Operator for checking the operating system’s service pack on Windows 8
<code>service_pack_major_version_number_8 (0)</code>	Specifies the major service pack version required for Windows 8 operating systems to be verified.
<code>service_pack_minor_version_number_8 (0)</code>	Specifies the minor service pack version required for Windows 8 operating systems to be verified.
<code>service_pack_version_operand_8 (“>=”)</code>	Operator for checking the operating system’s service pack on Windows 8.
<code>major_os_version_number_7 (6)</code>	Specifies the major version required for Windows 7 operating systems to be verified.
<code>minor_os_version_number_7 (1)</code>	Specifies the minor version required for Windows 7 operating systems to be verified.

Parameter	Description
<code>os_version_operand_7 ("=="</code>)	Operator for checking the operating system's service pack on Windows 7
<code>service_pack_major_version_number_7 (0)</code>	Specifies the major service pack version required for Windows 7 operating systems to be verified.
<code>service_pack_minor_version_number_7 (0)</code>	Specifies the minor service pack version required for Windows 7 operating systems to be verified.
<code>service_pack_version_operand_7 (">=")</code>	Operator for checking the operating system's service pack on Windows 7.
<code>major_os_version_number_vista (6)</code>	Specifies the major version required for Windows Vista operating systems to be verified.
<code>minor_os_version_number_vista (0)</code>	Specifies the minor version required for Windows Vista operating systems to be verified.
<code>os_version_operand_vista ("=="</code>)	Operator for checking the operating system's service pack on Windows Vista.
<code>service_pack_major_version_number_vista (1)</code>	Specifies the major service pack version required for Windows Vista operating systems to be verified.
<code>service_pack_minor_version_number_vista (0)</code>	Specifies the minor service pack version required for Windows Vista operating systems to be verified.
<code>service_pack_version_operand_vista (">=")</code>	Operator for checking the operating system's service pack on Windows Vista.
<code>os_version_mismatches ("Please upgrade your operating system")</code>	Message to be displayed in case of a non-verified configuration for the operating system's version/service pack. The operating system's version and service pack will not be checked if none of the parameters appear in the scv file.

ProcessMonitor

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

It is based on the process name, with an additional hash check option for running processes.

`ProcessName.exe (true | false)`

`ProcessName.exe (true;<SHA1 hash value>)`

For example: `calc.exe (true;9018A7D6CDBE859A430E8794E73381F77C840BE0)`

If the value is true, the client is compliant if this process is running.

If the value is false, the client is compliant if the process is not running.



Note - Checking the SHA1 hash value can impact performance.

RegMonitor

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



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

Parameter	Description
value (registry_value_path)	The path of a registry <code>DWORD</code> will be checked. The value should be an operator followed by a number, e.g. "Software\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\PatternVer>=414"
string (registry_string_path)	The path of a registry string will be checked. The string's value is compared to the given value, in the way that <code>DWORDs</code> are compared.
keynexist (registry_key_path)	The path of a registry key to be checked for exclusion. For the machine to be verified, the key should not exist.
keyexist (registry_key_path)	The path of a registry key to be checked for inclusion. For the machine to be verified, the key must exist.

Example: Script to check the version and service pack of Internet Explorer.

```

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

```

SCVMonitor

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

Parameter	Description
<code>scv_version(">=541000076")</code>	<p>SCV build-version of the SCV DLLs. This is not the same as the build number of Endpoint Security VPN.</p> <p>The string is an operator followed by the DLL's version number in the format "vvshhbbb". For example, if you want the DLL version to be at least 54.1.0.220, the syntax should be:</p> <pre>scv_version(">=541000220")</pre>

ScriptRun

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

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

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

WindowsSecurityMonitor

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

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

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

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

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

Parameter	Description
NetworkFirewallRequired	If it is set to true, a firewall is required. It queries the Windows Security Center to see if there is a Windows or third party firewall installed on the Endpoint machine.
NetworkFirewallInstalledPrograms	<p>Possible values:</p> <ul style="list-style-type: none"> • any - Checks if there is any firewall installed on the endpoint machine (registered in the Windows Security Center). • list of Firewalls separated by a ";" delimiter – Checks if one of the Firewalls on the list is installed on the endpoint machine. • none - Disables the check.
VirusProtectionRequired	<ul style="list-style-type: none"> • If it is set to true, an Anti-Virus product is required. It queries the Windows Security Center to see if there is an Anti-Virus product installed and running on the Endpoint machine. It also checks that the Anti-Virus is up to date and that it has automatic scanning configured.
VirusProtectionInstalledPrograms	<p>Checks which Anti-Virus program is installed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • any - Checks if there is any Anti-Virus installed on the endpoint machine (registered in the Windows Security Center). • list of Anti-Virus products separated by a ";" delimiter – Checks if one of the Anti-Virus products on the list is installed, on the endpoint machine. • none - Disables the check
SpywareProtectionRequired	If it is set to true, an Anti-Spyware protection and Unwanted Software product is required. It queries the Windows Security Center to see if there is an Anti-Spyware product installed on the Endpoint machine. It also checks that the Anti-Spyware is up to date and that it has automatic scanning configured.
SpywareProtectionInstalledPrograms	<p>Checks if there is an Anti-Spyware product installed on the Endpoint machine. Possible values:</p> <ul style="list-style-type: none"> • any - Checks if there is any Anti-Spyware installed on the endpoint machine (registered in the Windows Security Center). • list of Anti-Spyware products separated by a ";" delimiter – Checks if one of the Anti-Spyware products on the list is installed on the endpoint machine. • none - Disables the check <p>This check is not supported on Windows XP. If you configure it, it will run on Windows 7 and Vista but not on XP.</p>
WindowsUpdateRequired	<p>Queries the Windows Security Center to see if the Endpoint machine has Windows Automatic Updates configured.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • true - Enables the check. • false– Disables the check.
<CheckName>MismatchMessage	For each check, enter the message that users get if they are not compliant. For example, "You do not have a Firewall enabled. Enable a firewall or contact your administrator for help."

Parameter	Description
PassCheckWhenSecurityCenterIsUnavailable	<p>Can override the WindowsSecurityMonitor checks if the Windows Security Center is not working. Possible values:</p> <ul style="list-style-type: none"> • true - If a client fails the WindowsSecurityMonitor checks because of an internal error of the Microsoft WMI service (which reports from Windows Security Center), the fail is ignored. The client is considered compliant and can access the gateway. • false - (default) If there is an internal error of the Microsoft WMI service and a client fails the WindowsSecurityMonitor checks, it is considered non-compliant and cannot access the gateway. For security reasons, this is the default.
MinutesForWscsvToStart(x)	<p>If a client is not compliant because the wscsvc service did not start, it will be considered compliant for x minutes. If the wscsvc service does not start after x minutes, the client will be non compliant. Minutes are counted from when the computer boots.</p> <p>Enter a value (in minutes) for x.</p>

Finding Exact Product Names

You can include lists of products in the WindowsSecurityMonitor check for these parameters:

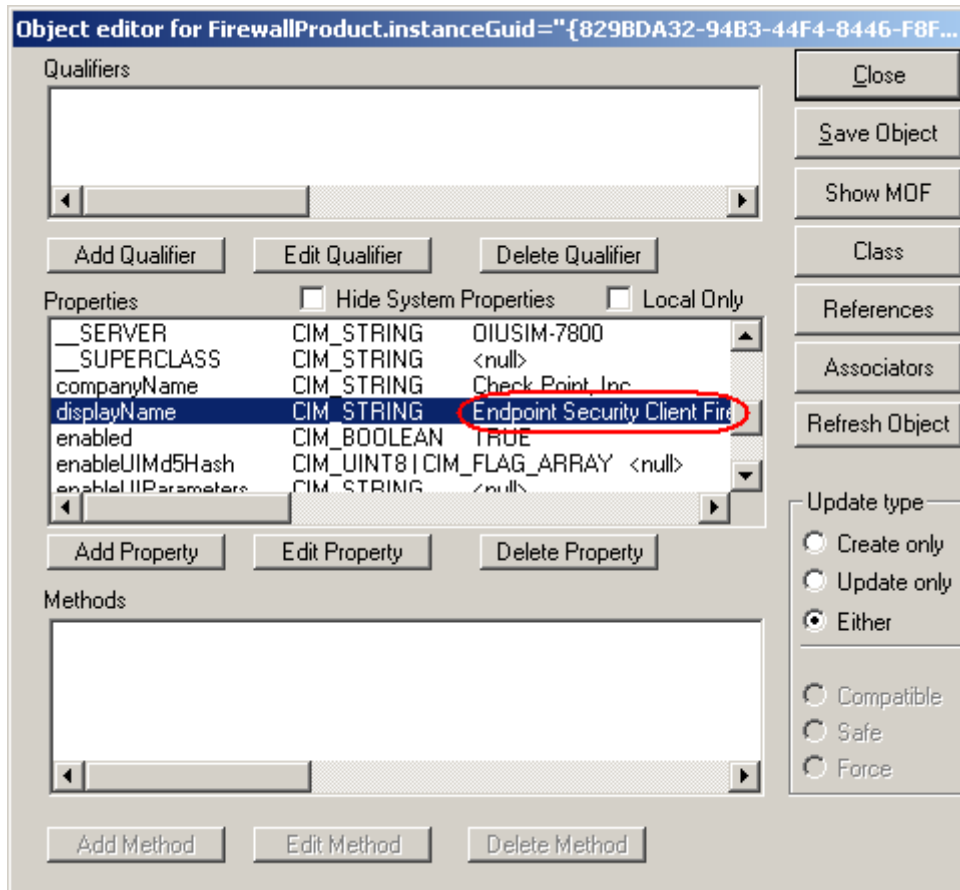
- NetworkFirewallInstalledPrograms
- VirusProtectionInstalledPrograms
- SpywareProtectionInstalledPrograms

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

To find names in the Windows Management Instrumentation Tester tool:

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

- In the **Object editor** window, scroll down to the **displayName** property. Copy the name listed and use that in the parameters of the check.



Example of a WindowsSecurityMonitor configuration

```

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

```

SCV Global Parameters

There are global features for the SCV checks.

Disconnect When Not Verified

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

1. On the Security Management Server, open `$FWDIR\conf\local.scv`.
2. In the `SCVGlobalParams` section, set the value of `disconnect_when_not_verified`.
 - **True** - A connected, non-compliant client is automatically disconnected from the VPN. A notification is shown to the user.
 - **False** - A connected, non-compliant client stays connected to the VPN. This is default.

Not Verified Script

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

1. On the Security Management Server, open `$FWDIR\conf\local.scv`.
2. In the `SCVGlobalParams` section, find `not_verified_script`.
3. In the value, put the name of the script.
 - You must supply the script to the client computers.
 - If necessary, you must make sure it is in the search path.
4. Set the value of `not_verified_script_run_show`.
 - **True** - The user will see the script running.
 - **False** - The script run will be hidden. (default)
5. Set the value `not_verified_script_run_admin`.
 - **True** - The script will run under the Remote Access Clients Service account with administrator permissions, even if the user does not have these permissions.
 - **False** - The script will run under the local user account permissions (default). If administrator permissions are necessary, the script will fail.
6. Set the value of `not_verified_script_run_always`.
 - **True** - The script runs every time the client becomes non-compliant.
 - **False** - The script runs the first time that the client becomes non-compliant. (default)

SCV Intervals

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

To change the interval in the global parameters:

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

If you set the value to 0 or enter an invalid value, such as a letter, the interval will be the default 20 seconds.

3. Install the desktop policy in SmartDashboard.
The change takes effect when a client connects.

Allow Clients without Firewall

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



Notes -

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

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

To enable Skip firewall enforcement in the global parameters:

1. On the Security Management Server, open `$FWDIR\conf\local.scv`.
2. In the `SCVGlobalParams` section, set the value of `skip_firewall_enforcement_check` to **true**.
3. Install the desktop policy in SmartDashboard.
The change takes effect when a client connects.

Allow Clients without SCV

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

To enable Allow non SCV Clients in the global parameters:

1. On the Security Management Server, open `$FWDIR\conf\local.scv`.
2. In the `SCVGlobalParams` section, set the value of `allow_non_scv_clients` to **true**.
3. Install the desktop policy in SmartDashboard.

The change occurs when a client connects.

Enforcing the SCV Checks

To enforce a specified SCV check from versions before E75.10:

- Set the SCV parameters in **SCVNames**.
- Include the name of the check in **SCVPolicy**.

To enforce SCV checks from version E75.10 or later, such as WindowsSecurityMonitor:

- Set the SCV parameters in **SCVEpsNames**.
- Include the name of the check in **SCVEpsPolicy**.

Sample local.scv Configuration File

You must maintain the same indentation format.

```
(SCVObject
  :SCVNames (
    : (user policy scv
      :type (plugin)
      :parameters (
        )
      )
    : (BrowserMonitor
      :type (plugin)
      :parameters (
        :browser_major_version (5)
        :browser_minor_version (0)
        :browser_version_operand (">=")
        :browser_version_mismatchmessage ("Please upgrade your
Internet browser.")
        :intranet_download_signed_activex (disable)
        :intranet_run_activex (disable)
        :intranet_download_files (disable)
        :intranet_java_permissions (disable)
        :trusted_download_signed_activex (disable)
        :trusted_run_activex (disable)
        :trusted_download_files (disable)
        :trusted_java_permissions (disable)
        :internet_download_signed_activex (disable)
        :internet_run_activex (disable)
        :internet_download_files (disable)
        :internet_java_permissions (disable)
        :restricted_download_signed_activex (disable)
        :restricted_run_activex (disable)
        :restricted_download_files (disable)
        :restricted_java_permissions (disable)
        :send_log (alert)
        :internet_options_mismatch_message ("Your Internet
```

```

browser settings do not meet policy requirements\nPlease check the
following settings:\n1. In your browser, go to Tools -> Internet Options
-> Security.\n2. For each Web content zone, select custom level and
disable the following items: Download signed ActiveX, Run ActiveX
Controls, Download Files and Java Permissions.")
)
)
: (OsMonitor
  :type (plugin)
  :parameters (
    :os_version_mismatchmessage ("Please upgrade your
operating system.")
    :enforce_screen_saver_minutes_to_activate (3)
    :screen_saver_mismatchmessage ("Your screen saver
settings do not meet policy requirements\nPlease check the following
settings:\n1. Right click on your desktop and select properties.\n2.
Select the Screen Saver tab.\n3. Under Wait choose 3 minutes and check
the Password Protection box.")
    :send_log (alert)
    :major_os_version_number_9x (4)
    :minor_os_version_number_9x (10)
    :os_version_operand_9x (">=")
    :service_pack_major_version_number_9x (0)
    :service_pack_minor_version_number_9x (0)
    :service_pack_version_operand_9x (">=")
    :major_os_version_number_nt (4)
    :minor_os_version_number_nt (0)
    :os_version_operand_nt ("==")
    :service_pack_major_version_number_nt (5)
    :service_pack_minor_version_number_nt (0)
    :service_pack_version_operand_nt (">=")
    :major_os_version_number_2k (5)
    :minor_os_version_number_2k (0)
    :os_version_operand_2k ("==")
    :service_pack_major_version_number_2k (0)
    :service_pack_minor_version_number_2k (0)
    :service_pack_version_operand_2k (">=")
    :major_os_version_number_xp (5)
    :minor_os_version_number_xp (1)
    :os_version_operand_xp ("==")
    :service_pack_major_version_number_xp (0)
    :service_pack_minor_version_number_xp (0)
    :service_pack_version_operand_xp (">=")
    :major_os_version_number_2003 (5)
    :minor_os_version_number_2003 (2)
    :os_version_operand_2003 ("==")
    :service_pack_major_version_number_2003 (0)
    :service_pack_minor_version_number_2003 (0)
    :service_pack_version_operand_2003 (">=")
  )
)
)
: (ProcessMonitor
  :type (plugin)
  :parameters (
    :calc.exe (false)
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Please make sure calc.exe is
not running!")
    :end_admin (admin)
  )
)
)
: (groupmonitor
  :type (plugin)
  :parameters (

```

```

        :begin_or (or1)
            :begin_and (1)
                :bultin\administrator" (false)
                :BUILTIN\Users" (true)
            :end (1)
            :begin_and (2)
                :bultin\administrator" (true)
                :BUILTIN\Users" (false)
            :end (and2)
        :end (or1)
    :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("You are using SecureClient
with a non-authorized user.\nMake sure you are logged on as an authorized
user.")
        :securely_configured_no_active_user (false)
    :end (admin)
)
)
: (HotFixMonitor
    :type (plugin)
    :parameters (
        :147222 (true)
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Please install security patch
Q147222.")
    :end (admin)
)
)
: (AntiVirusMonitor
    :type (plugin)
    :parameters (
        :type ("Norton")
        :Signature (">=20020819")
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Please update your AntiVirus
(use the LiveUpdate option).")
    :end (admin)
)
)
: (HWMonitor
    :type (plugin)
    :parameters (
        :cputype ("GenuineIntel")
        :cpumodel ("9")
        :cpufamily ("6")
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Your machine must have
an\nIntel(R) Centrino(TM) processor installed.")
    :end (admin)
)
)
: (ScriptRun
    :type (plugin)
    :parameters (
        :exe ("VerifyScript.bat")
        :begin_admin (admin)
        :send_log (alert)
        :mismatchmessage ("Verification script has
determined that your configuration does not meet policy requirements.")
    :end (admin)
)
)

```

```

)
: (RegMonitor
  :type (plugin)
  :parameters (
    :value ("Software\TrendMicro\PC-
cillinNTCorp\CurrentVersion\Misc.\PatternVer>=414")
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Please update your AntiVirus
(use the LiveUpdate option).")
    :end (admin)
  )
)
: (SCVMonitor
  :type (plugin)
  :parameters (
    :scv_version ("54014")
    :begin_admin (admin)
    :send_log (alert)
    :mismatchmessage ("Please upgrade your Secure
Configuration Verification products package.")
    :end (admin)
  )
)
: (sc_ver_scv
  :type (plugin)
  :parameters (
    :Default_SecureClientBuildNumber (52032)
    :Default_EnforceBuildOperand ("==")
    :MismatchMessage ("Please upgrade your SecureClient.")
    :EnforceBuild_9X_Operand (">=")
    :SecureClient_9X_BuildNumber (52030)
    :EnforceBuild_NT_Operand ("==")
    :SecureClient_NT_BuildNumber (52032)
    :EnforceBuild_2K_Operand (">=")
    :SecureClient_2K_BuildNumber (52032)
    :EnforceBuild_XP_Operand (">=")
    :SecureClient_XP_BuildNumber (52032)
  )
)
)
)
:SCVEpsNames (
  : (WindowsSecurityMonitor
    :type (plugin)
    :parameters (
      :VirusProtectionRequired (true)
      :VirusProtectionRequiredMismatchMessage ("Please verify
that your virus protection is up to date and virus scanning is on.")
      :VirusProtectionInstalledPrograms ("Kaspersky Anti-
Virus")
      :VirusProtectionInstalledProgramsMismatchMessage
("Please verify that the anti-virus of Kaspersky Anti-Virus is
installed.")
      :WindowsUpdateRequired (false)
      :WindowsUpdateRequiredMismatchMessage ()
      :SpywareProtectionRequired (true)
      :SpywareProtectionRequiredMismatchMessage ("Please
verify that your spyware protection is turned on.")
      :SpywareProtectionInstalledPrograms (any)
      :SpywareProtectionInstalledProgramsMismatchMessage
("There is no anti-spyware program installed on the machine.")
      :NetworkFirewallRequired (true)
      :NetworkFirewallRequiredMismatchMessage ("Please verify
the your network firewall is turned on.")
      :NetworkFirewallInstalledPrograms ("Kaspersky Anti-

```

```

Virus")
        :NetworkFirewallInstalledProgramsMismatchMessage
("Please verify that the firewall of Kaspersky Anti-Virus is installed on
the machine.")
    )
)
)
:SCVEpsPolicy (
: (WindowsSecurityMonitor)
)
:SCVPolicy (
        : (ProcessMonitor)
)
)
:SCVGlobalParams (
:enable_status_notifications (false)
:status_notifications_timeout (10)
:disconnect_when_not_verified (false)
:skip_firewall_enforcement_check (false)
:block_connections_on_unverified (false)
:scv_policy_timeout_hours (168)
:enforce_ip_forwarding (false)
:not_verified_script ("")
:not_verified_script_run_show (false)
:not_verified_script_run_admin (false)
:not_verified_script_run_always (false)
:allow_non_scv_clients (false)
)
)
)

```

Deploying a Third Party SCV Check

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

We recommended that you add the DLL to an MSI package with the Check Point MSI Packaging tool utility ("[Editing an MSI Package with CLI](#)" on page 36). When clients install the MSI they automatically get the DLL.

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

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

To activate a third party SCV check:

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

Chapter 6

The Configuration File

In This Chapter

Editing the TTM File	103
Centrally Managing the Configuration File	103
Understanding the Configuration File	104

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

Editing the TTM File

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

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



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

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

To activate changes in the TTM file:

1. Edit and save the file.
2. Install the policy from SmartDashboard or the CLI of each gateway:
 - In SmartDashboard, select **Policy > Install** and install **Network Security** on each changed gateway.
 - Run `cpstop` and `cpstart` from the CLI of each changed gateway.



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

Centrally Managing the Configuration File

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



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

To centrally manage the configuration file on non-legacy gateways:

1. On the gateway, save a backup of `$FWDIR/conf/trac_client_1.ttm`.
2. From the gateway, copy `trac_client_1.ttm` to the server.
3. Open `$FWDIR/conf/fwrl.conf` and find the `% SEGMENT FILTERLOAD` section.
4. In the NAME section, add this line:
`NAME = conf/trac_client_1.ttm;DST = conf/trac_client_1.ttm;`

This copies the file to the Remote Access Clients gateways each time that you install the policy on the gateways.

5. Save the file.
6. In SmartDashboard, install the policy on all gateways.

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

The procedure above does not apply to the legacy gateways managed with a compatibility pack. For example, R71 managed by R75.

To centrally manage the configuration file on legacy gateways:

1. Open `fwrl.conf` in the relevant compatibility pack directory:
`/opt/CP###CMP-$$$/conf/`, where `###` is the target gateway version, and `$$$` is the current SMC version.
 For example, for an R77 gateway managed by an R75.20 SMC, the directory would be `/opt/CPR77CMP-R75.20`.
2. Find the `% SEGMENT FILTERLOAD` section.
3. In the `NAME` section, add this line:
`NAME = conf/trac_client_1.ttm;DST = conf/trac_client_1.ttm;`
 This copies the file to the Remote Access Clients gateways each time that you install the policy on the gateways.
4. Save the file.
5. Create a symbolic link to the TTM file in `$FWDIR/conf/` by running this command:
`ln -s $FWDIR/conf/trac_client_1.ttm trac_client_1.ttm`
6. Install the policy on the gateway

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

The behavior for each attribute is decided in this way:

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

- If the attribute is not configured in the client GUI, it is taken from the `trac.defaults` file on each client.

Example:

```
:enable_password_caching (  
  :gateway (  
    :default (client_decide)  
  )  
)
```

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

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

Configuration File Parameters

See sk75221 (<http://supportcontent.checkpoint.com/solutions?id=sk75221>) for an updated list of parameters for the configuration file.

Chapter 7

Monitoring and Troubleshooting

In This Chapter

SmartView Tracker and Remote Access Clients	106
Collecting Logs	107
Remote Access Clients Files	108
"Unsupported Services" Message	109
Configuring No-Router Environments	109
Connection Terminates	110
Troubleshooting the Firewall	110
Troubleshooting SCV	117
Traffic Dropped for Anti-spoofing	118
MEP	118

SmartView Tracker and Remote Access Clients

To see alerts from Remote Access Clients:

1. Open SmartView Tracker.
2. In **Network & Endpoint**, open **Network Security Blades > IPSEC VPN Blade**.

No.	Date	Time	Interface	Origin	Type	Action	Service
1	11Nov2008	11:00:28	Desktop	Alaska_cluster	Alert		
2	11Nov2008	22:10:45	Desktop	Alaska_cluster	Alert		
3	12Nov2008	4:04:16	Desktop	California_GW	Alert		
4	14Nov2008	3:42:05	Desktop	California_GW	Alert		
5	14Nov2008	4:12:00	Desktop	Delaware_cluster	Alert		
6	15Nov2008	10:03:59	Desktop	Georgia_GW	Alert		
7	19Nov2008	13:07:47	Desktop	Georgia_GW	Alert		
8	22Nov2008	19:46:08	E100B2	Alaska_cluster	Alert	Drop	nbname
9	22Nov2008	19:46:09	Desktop	California_GW	Alert	Drop	
10	22Nov2008	19:46:09	E100B2	Alaska_cluster	Alert	Drop	nbname
11	22Nov2008	19:46:09	Desktop	California_GW	Alert	Drop	
12	22Nov2008	19:46:10	E100B2	Alaska_cluster	Alert	Drop	nbdatagram

3. Double-click an item to open the **Record Details** window and see more data.

Log Info		Rule	
Date	11Nov2008	Action	
Time	22:10:45	Rule	---
Number	2	Current Rule Number	---
Type	! Alert	Rule Name	---
Origin	Alaska_cluster	User	sdavid

Traffic		More	
Destination	---	Information message: Failed to load Desktop Security Policy Standard site_name: Alaska	
Service	---		
Protocol	---		
Interface	Desktop		
Source Port	---		

Policy	
Policy Name	---
Policy Date	---
Policy Management	---

Collecting Logs

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

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

To define a default email address for log files:

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

```

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

```

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

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

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

To collect logs on a client:

1. Right-click the client icon and select **VPN Options**.
2. Open the **Advanced** tab.
3. Make sure **Enable Logging** is selected.
4. Reproduce the issue.
5. Click **Collect Logs**.
This takes some time.

Troubleshooting Log Collection

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

Remote Access Clients Files

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

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	The Remote Access Clients CLI (" Remote Access Clients Command Line " on page 125).	
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 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.	<p>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.</p> <p>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.</p>
vna.sys	driver	
cpgina.log, cpplap.log	Logs for Remote Access Clients support for Windows SDL by GINA and PLAP.	

Filename	Description	Notes
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.
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.

"Unsupported Services" Message

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	<ol style="list-style-type: none"> 1. Open <code>trac.log</code>. 2. Find: <code>ConvertRule: ERROR - BuildProtocolString failed!!</code> 3. Go up two lines and find the rule number: <code>ConvertRule: rule = rule-<number>, start converting...</code> 4. Open <code>desktop_policy.ini</code> and find the rule number. 5. In the <code>svc</code> section, find the services of the rule that are not supported. (For example, <code>dcerpc</code> services are not supported.) 6. Open SmartDashboard, find the rule in the Desktop policy, and remove the unsupported service.

Configuring No-Router Environments

You must configure the server in SmartDashboard if there is no router between the gateway and the Remote Access Clients client (for example, in a lab environment).

To configure Remote Access Clients to operate without a router:

1. In SmartDashboard, open the properties of the Remote Access Clients gateway.
2. Open **Office Mode**:
 - **R71: IPSEC VPN > Office Mode**
 - **NGX R65 and R70: Remote Access > Office Mode**

3. Select the **Multiple Interfaces** option: **Support connectivity enhancement for gateways with multiple external interfaces**

Connection Terminates

If all client connections stop at a given interval (default is 15 minutes), the DHCP server might be configured to use the lowest IP lease timeout.

To repair this issue:

1. In SmartDashboard, open the Gateway Properties window of the Remote Access Clients gateway.
2. Open Office Mode:
 - R71: **IPSec VPN > Office Mode**
 - R70 and NGX R65: **Remote Access > Office Mode**
3. Click **Offer Office Mode to group** or **Allow Office Mode to all users**.
4. Click **Optional Parameters**.
5. Increase the value of **IP lease duration**.
6. Click **OK**.
7. Install Policy.

Troubleshooting the Firewall

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

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 E80.41 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	<code>packetmon -h</code>

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

-f file	
Purpose	<p>This option filters packets according to INSPECT expressions in a given file. To use pre-defined INSPECT macros, the given file must include the <code>'#include "fwmonitor.def"'</code> directive.</p> <p>Note: The <code>-f</code> option can not be used with the <code>-e</code> option.</p>
Example	<code>packetmon -f inspect.dat</code>
	<p>Inspect.dat contents:</p> <pre>#include "fwmonitor.def" tcpport(23), accept;</pre>

-f -	
Purpose	<p>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:</p> <pre>#include "fwmonitor.def"</pre> <p>To stop command input and start packet inspection based on the given input, enter <code>Ctrl-Z+<Enter></code> at a new line.</p> <p>Note: The <code>-f -</code> option can not be used with the <code>-e</code> option.</p>
Example	<code>packetmon -f -</code>
	<p>Standard input contents:</p> <pre>#include "fwmonitor.def" tcpport(23), accept; Ctrl-Z+<Enter></pre>

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

-l len	
Purpose	Limits packet capture length to the given <code>len</code> bytes. Note: <code>len</code> indicates number of bytes to capture starting at the IP header. Regardless of the <code>len</code> value, the MAC header is always captured.
Example	<code>packetmon -l 20</code>
Default	If the <code>-l</code> option is not given, all packet data is captured
Comment	<ul style="list-style-type: none"> 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 <code>packetmon</code> 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	<p>By default <code>packetmon</code> captures packets before and after firewall inspection. The <code>-m</code> option lets you to specify capture on:</p> <ul style="list-style-type: none"> <code>i</code> Inbound packets before firewall inspection. <code>I</code> Inbound packets after firewall inspection. <code>o</code> Outbound packets before firewall inspection <code>O</code> Outbound packets after firewall inspection <p>The mask can be a combination of the above.</p>
Example	<code>packetmon -m IO</code>
Default	Not specifying the <code>-m</code> option is the same as running: <code>packetmon -m iIoO</code>

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

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

-ci count / -co count	
Purpose	<p>This option limit the number of packets being captured. This is useful when you need to troubleshoot a firewall handling large amounts of traffic.</p> <ul style="list-style-type: none"> <code>-ci</code> Defines how many inbound packets to capture <code>-co</code> Defines how many outbound packets to capture
Examples	<pre>packetmon -ci 5 packetmon -ci 3 -co 10</pre>

-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	<pre>packetmon -I</pre>
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	<pre>packetmon -d</pre>

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	<code>packetmon -r</code>

-T	
Purpose	This option prints the time stamp for each packet.
Example	<code>packetmon - T</code>

-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	<code>packetmon -i > output.log</code>

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

Macro	Purpose	Example
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
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

Macro	Purpose	Example
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

Troubleshooting SCV

"file is corrupt"

Symptom	Client shows an error message: <code>Compliance Policy file is corrupt. Please contact your system administrator.</code>
Scenario	An SCV check defined in the SCVPolicy section is not defined in the local.scv policy, SCVNames section.
Solution	Make sure that the SCVNames section includes all the checks that are to be run on clients.

"unsupported format"

Symptom	Client shows an error message: <code>Compliance Policy is in an supported format</code>
----------------	---

Scenario	Can be one of these issues: <ul style="list-style-type: none"> • There is no SCVObject section in the local.scv policy file. • An SCV plug-in configured in the local.scv policy file does not exist on the client computer, or it has a functionality issue. • The SCV Check type as defined in the local.scv policy is not a plug-in. • The local.scv policy context has an incorrect format. • The local.scv file was edited on an operating system that is different than the gateway operating system and the file was saved in an encoding that the gateway cannot read.
Solution	See the SCV section in this Administration Guide and follow the instructions to edit and maintain the local.scv file.

"policy is not updated"

Symptom	Client shows an error message: <code>Compliance policy is corrupt. Please connect again to update the policy.</code>
Scenario	The policy enforced on the client computer is not updated with the latest security policy defined on the gateway.
Solution	Connect the client computer again to the gateway. The client pulls the latest security policy when it connects to the gateway.

Traffic Dropped for Anti-spoofing

Symptom	Traffic is dropped.
Scenario	For environments in which clients connect to the VPN community from internal interfaces (and the VPN community is behind an external interface), Anti-spoofing must be configured differently.
Solution	Include the office mode network in the internal interface Anti-spoofing settings.

MEP

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

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

Chapter 8

Advanced Configurations

In This Chapter

[Overlapping Encryption Domains](#)

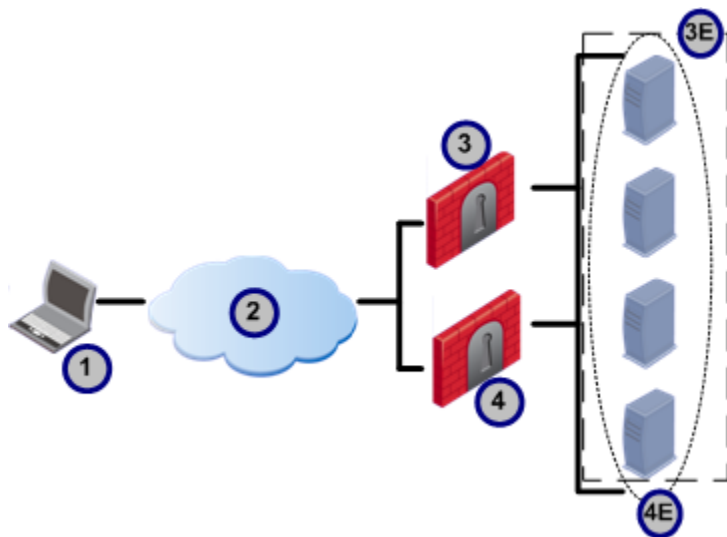
119

Overlapping Encryption Domains

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

Full Overlap

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



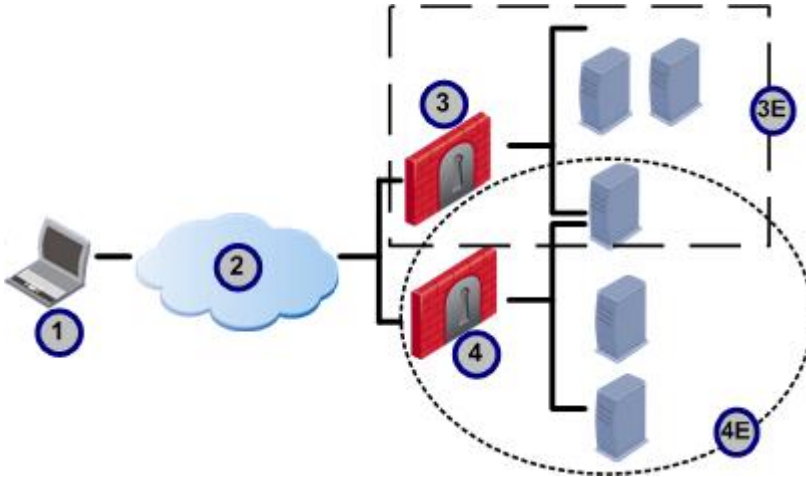
Item	Description
1	Remote Access Client
2	Internet
3	Gateway A
3E	Encryption Domain for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B

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.

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

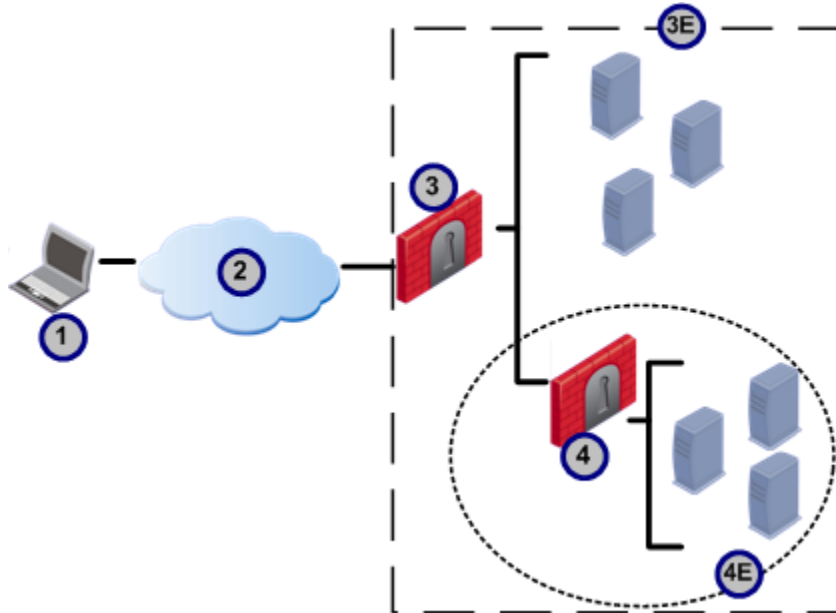
Proper Subset

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.

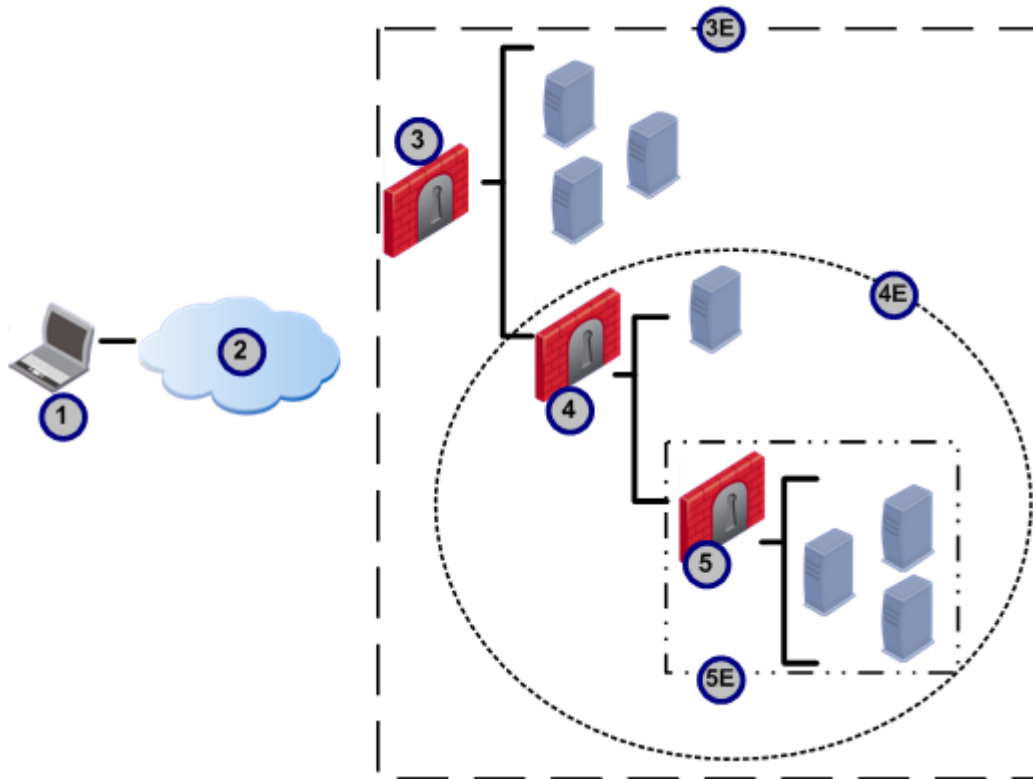
For example, in the picture below, Gateway B is a proper subset of Gateway A.



Item	Description
1	Remote Access Client
2	Internet
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 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
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:

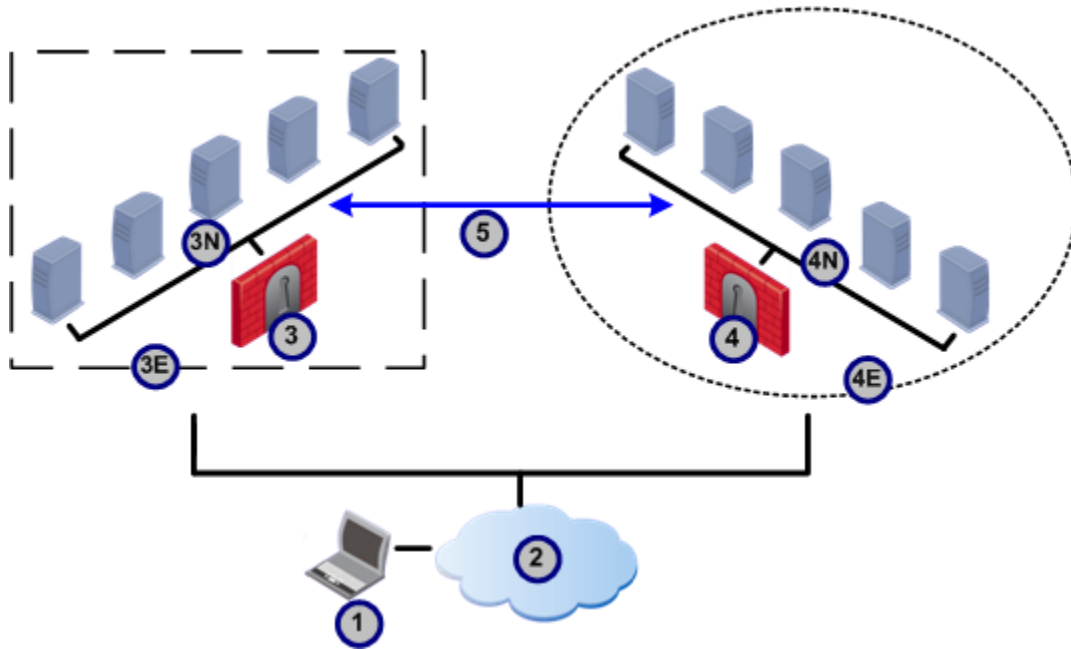
Host	Connects to
Hosts in Gateway C's encryption domain	Gateway C
Host only in gateway B's encryption domain and not in another encryption domain	Gateway B
All other hosts	Gateway A

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.

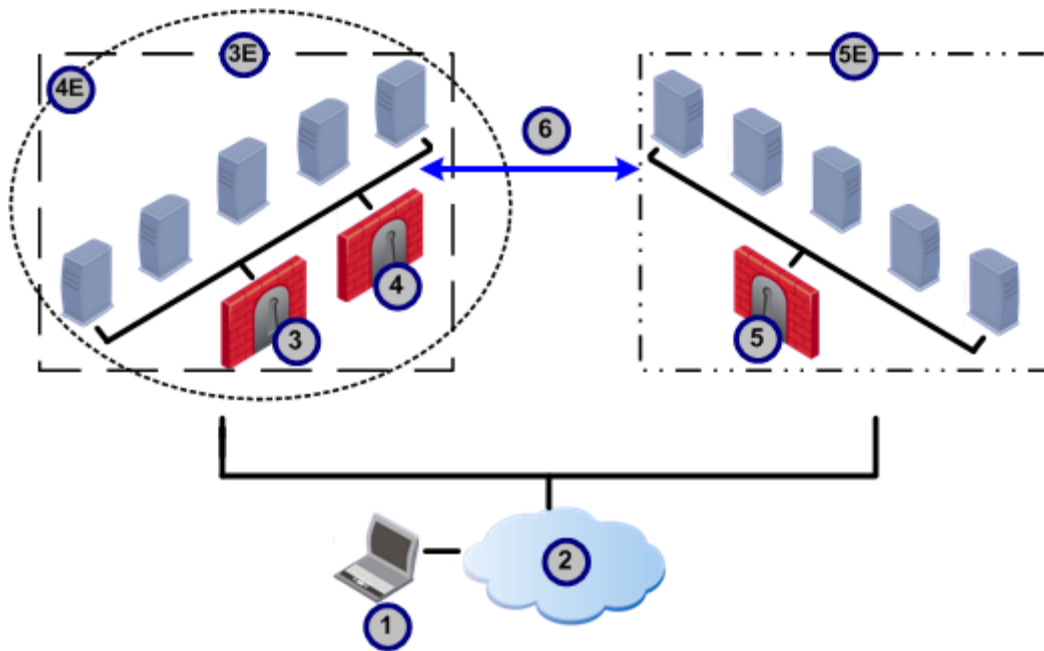


Item	Description
1	Remote Access Client
2	Internet
3	Gateway A
3E	Encryption Domain for Gateway A
3N	Internal Network for Gateway A
4	Gateway B
4E	Encryption Domain for Gateway B
4N	Internal Network for Gateway B
5	Dedicated Link

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.

Appendix A

Remote Access Clients Command Line

In This Appendix

[Using the Command Line](#)

125

[CLI Commands](#)

125

Using the Command Line

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

To use the command line:

1. Open a terminal: **Start > Run > cmd**



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

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

CLI Commands

These commands can be used for Remote Access Clients.

change_p12_pwd

change_p12_pwd

Description Changes the password of a p12 certificate.

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

Arguments	Args	Description
	-s	name of the site
	-f	pathname to the certificate file
	-o	old password for the certificate
	-n	new password for the certificate

change_p12_pwd

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

You can use the feature interactively:

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

connect**connect**

Description Connects the local client to a site.

Syntax

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

Arguments

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

Example

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



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

connectgui

connectgui

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

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

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

create

create

Description Creates a new site and defines its authentication method.

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

Arguments

Args	Description
-s	name of the site
-a	Valid values: <ul style="list-style-type: none"> • username-password • certificate • pl2-certificate • challenge-response • securIDKeyFob • securIDPinPad • SoftID

Example

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

delete

delete

Description Deletes a site definition.

Syntax `trac delete -s <site>`

Arguments

Args	Description
-s	name of the site

Example

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

disable_log

disable_log

Description	Stops logging.
Syntax	<code>trac disable_log</code>
Arguments	none

disconnect

disconnect

Description	Disconnects the local client from the current connection.
Syntax	<code>trac disconnect [-g <gateway>]</code>

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

enable_log

Description	Enables logging.
Syntax	<code>trac enable_log</code>
Arguments	none

enroll_capi

enroll_capi

Description	Enrolls a CAPI certificate.
Syntax	<code>trac enroll_capi -s <site> -r <key> [-i <providerindex> -l <keylength> -sp <strongkeyprotection>]</code>

enroll_capi

Arguments	Args	Description
	-s	name or IP address of the site
	-r	registration key
	-i	where to store the certificate (If you do not enter this in the command, the output shows the options.)
	-l	length of the registration key
	-sp	whether strong key protection is used (Valid values: "true" or "false")

Example

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

enroll_p12**enroll_p12**

Description Enrolls a p12 certificate.

Syntax

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

Arguments

Args	Description
-s	name of the site
-f	pathname to the certificate file
-p	password for the certificate
-r	registration key
-l	length of the key

Example

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

firewall**firewall**

Description Enables or disables the Desktop firewall

Syntax

```
firewall -st enable|disable
```

Arguments None

help

help

Description Outputs help on the CLI or for a command.

Syntax `trac help | h`

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

hotspot_reg

hotspot_reg

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

Syntax `hotspot_reg`

Arguments none



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

info

info

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

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

Arguments

Args	Description
-s	name of the site If given, only gateways and tunnel information for this site are shown.

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

List

List

Description Shows certificate subject names stored in the CAPI.

Syntax `trac List`

Arguments none

List

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

Log

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

Syntax trac Log

Arguments none

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

renew_capi

renew_capi

Description Renews a capi certificate.

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

Arguments

Args	Description
-s	name of the site
-d	certificate subject name
-l	length of the registration key
-sp	if strong key protection is used (Valid values: "true" or "false")

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

renew_p12

renew_p12

Description Renews a p12 certificate.

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

renew_p12

Arguments	Args	Description
	-s	name of the site
	-f	pathname for the certificate file
	-p	password for the certificate
	-l	length of the key

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

set_proxy_settings**set_proxy_settings**

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

Arguments	Args	Description
	-m mode	one of no_proxy manual auto <ul style="list-style-type: none"> 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)
	-h -p	hostname and port of the proxy This can be set only when the proxy mode is manual
	-u -p	username and password credentials This can be set only when the proxy mode is not no_proxy

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

start**Start**

Description Starts the Remote Access Clients service.

Syntax `trac start`

Arguments none



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

stop

Stop

Description Stops the Remote Access Clients service.

Syntax `trac stop`

Arguments none



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

Ver

Ver

Description Shows the version of the client.

Syntax `trac Ver`

Arguments none

sdl

sdl

Description Enable or disable Secure Domain Logon (SDL).

Syntax `trac sdl -st <state>`

Arguments

Args	Description
-st	SDL state – "enable" / "disable"

Example
`trac sdl -st enable`
`trac sdl -st disable`

userpass

userpass

Description For ATM clients, sets the username and password.

Syntax `trac userpass -s <sitename> -u <username> -p <password>`

Example To set username and password:

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

To delete username and password:

```
userpass -s <sitename>
```

certpass

certpass

Description For ATM clients, sets the certificate path and password.

Syntax `trac certpass -s <sitename> -f <certificate filename> -p <password>`

Example To set username and password:

```
trac certpass -s <sitename> -f <certificate filename> -p <password>
```

To delete certificate credentials:

```
certpass -s <sitename>
```

Appendix B

Creating a DLL file to use with SAA

In This Appendix

OPSEC - Open Platform for Security	135
Overview of SAA	135
How Does SAA Work	135
Summary of OPSEC API Functions	136

OPSEC - Open Platform for Security

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

Overview of SAA

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

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

How Does SAA Work

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

Scenario with a non-SAA Authentication Method

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

1. Hugo initiates a connection to a host in the London gateway's encryption domain.
2. The Check Point client sends Hugo's username to the Security Management Server that also manages the Check Point clients.
3. The Security Management Server challenges Hugo to authenticate himself according to the authentication scheme configured for that site.
4. Hugo enters the response to the challenge (usually a password).
5. If the response was correct, the Check Point client and the Security Management Server exchange a session key. This key is used to encrypt the data connection.

Scenario with SAA

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

1. The Authentication Agent exports a small number of functions in an Authentication DLL file (located on the user's machine).
2. These functions let the client forward the Security Management server's challenges to the Authentication Agent on Hugo's machine.
3. The client forwards the responses from the Authentication Agent back to the Security Management Server.
4. When Hugo initiates a connection to a host in the London gateway's encryption domain the Check Point client calls the appropriate functions in the Authentication DLL rather than displaying the standard login windows.
5. When the Security Management Server decides to accept or deny the connection, a status indicator is sent to the Authentication Agent.
6. The Check Point client and the Security Management Server exchange a session key. This key is used to encrypt the data connection.



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

Important Note on Working with SAA

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

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

Summary of OPSEC API Functions

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

To understand the advantages of Version 2, see the legacy Secure Authentication API Specification (<http://downloads.checkpoint.com/dc/download.htm?ID=7389>).



Note - The function prototypes are defined in the file `authplugin.h` which can be found on the OPSEC Desktop SDK (<http://downloads.checkpoint.com/dc/download.htm?ID=7390>).

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.

API Function	Version (Ver)	Summary of Functionality
Username	For Ver 1 and Ver 2	Supplies the username to be used by the client to authenticate with the gateway for SAA Challenge/Response authentication.
UserNameAndPassword or UserNameAndPasswordVer2	UserNameAndPassword - Ver 1 UserNameAndPasswordVer 2 - Ver 2	Supplies the username and password to be used by the client to authenticate with the gateway for SAA Username/Password authentication.
Response	For Ver 1 and Ver 2	The client gives the Authentication Agent the challenge that it gets from the gateway. The Authentication Agent returns a response that the client sends back to the gateway.
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 <code>UserName</code> function.
usernameAndPasswordVer2Proc	Out	The address of the Authentication Agent's <code>UserNameAndPasswordVer2</code> function.
responseProc	Out	The address of the Authentication Agent's <code>Response</code> function.
goingdownProc	Out	The address of the Authentication Agent's <code>GoingDown</code> function.
authCompletedProc	Out	The address of the Authentication Agent's <code>AuthCompleted</code> function.
releaseContextProc	Out	The address of the Authentication Agent's <code>ReleaseContext</code> 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 <code>UserName</code> function.
usernameAndPassword	Out	The address of the Authentication Agent's <code>UserNameAndPassword</code> function.
Response	Out	The address of the Authentication Agent's <code>Response</code> function.
Terminate	Out	The address of the Authentication Agent's <code>Terminate</code> function.
Goingdown	Out	The address of the Authentication Agent's <code>GoingDown</code> 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 Version 1 and Version 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- it uses it directly.

UserName

For Version 1 and Version 2.

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

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

Prototype

```
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 <code>username</code> should be copied.
usernameLength	In Out	In - Length of the buffer allocated for <code>username</code> . Out - If <code>username</code> is longer than the specified length, the function should return <code>PLUGIN_DATA_TOO_LONG</code> 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 <code>Response</code> .

Return Values

`PLUGIN_OK` if successful.

`PLUGIN_ABORT` if the client should take over the authentication.

`PLUGIN_DATA_TOO_LONG` if the buffer specified by `username` is not long enough.

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

UsernameAndPassword or UserNameAndPasswordVer2

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

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

UserNameAndPasswordVer2

Prototype

```
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 <code>username</code> should be copied.
usernameLength	In Out	In - Length of the buffer allocated for <code>username</code> . Out - If <code>username</code> is longer than the specified length, the function should return <code>PLUGIN_DATA_TOO_LONG</code> 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 <code>password</code> . Out - If <code>password</code> is longer than the specified length, the function should return <code>PLUGIN_DATA_TOO_LONG</code> 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 <code>Response</code> .

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 gateway. The Authentication Agent shows the challenge to the user. The user enters a response to the challenge.

The Authentication Agent returns the user's `Response` back to the client, which forwards it to the gateway.

Prototype

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

Arguments

Argument	In/Out	Meaning
context	In	The context as provided by <code>Username</code>
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 <code>response</code> . Out - If username is longer than the specified length, the function should return <code>PLUGIN_DATA_TOO_LONG</code> 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 <code>Username</code> or <code>UsernameAndPassword</code> .

Argument	In/Out	Meaning
status	In	The status of the authentication. One of these values: <ul style="list-style-type: none"> • PLUGIN_DONE_SUCCESS - authentication was successful • PLUGIN_DONE_FAILED - authentication failed • PLUGIN_DONE - authentication has been cancelled for example, the password has expired or been erased.
message	In	The termination message, if provided by the authentication server.

Return Values

PLUGIN_OK if successful.

PLUGIN_CANCEL if the input does not make sense.

AuthCompleted

For Version 2

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

AuthCompleted

Prototype

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

Arguments

Argument	In/Out	Meaning
context	In	The context as provided by <code>Username</code> or <code>UsernameAndPassword</code> .
status	In	The status of the authentication. One of these values: <ul style="list-style-type: none"> • PLUGIN_DONE_SUCCESS - authentication was successful • PLUGIN_DONE_FAILED - authentication failed • PLUGIN_DONE - authentication has been cancelled for example, the password has expired or been erased.
message	In	The termination message, if provided by the authentication server.

Return Values

PLUGIN_OK if successful.

PLUGIN_CANCEL if the input does not make sense.

ReleaseContext

For version 2.

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

Prototype

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

Arguments

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

Return Values

None.

GoingDown

For Version 1 and Version 2

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

Prototype

```
void GoingDown()
```

Arguments

There are no arguments.

Return Values

None.

InvalidateProcCB

For Version 1 and Version 2

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

Prototype

```
void InvalidateProcCB()
```

Arguments

There are no arguments.

Return Values

None.