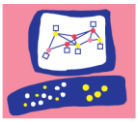


Check Point®
SOFTWARE TECHNOLOGIES LTD.

Discovery

NGX R65

Migration Guide

26 May 2010

More Information

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

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

Feedback

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

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Discovery NGX R65 Migration Guide).

Contents

Chapter 1

Introduction to Discovery

In This Chapter

Discovery Overview

Discovery is a lightweight remote access client that supplies seamless, secure IPSec VPN connectivity to remote resources. It works with physical Security Gateways and VSX Virtual Systems.

Discovery is intended to replace Check Point's existing remote access client SecureClient.

Note - VSX Virtual Systems do not support these Discovery features:

- Secure Configuration Verification (SCV)
- Desktop Firewall
- Log Uploads

Why You Should Migrate to Discovery

Check Point recommends that all customers upgrade from SecureClient to Discovery as soon as possible, because Discovery has these capabilities:

- Supports both 32 and 64 bit Windows Vista and Windows 7
- Uses less memory resources than SecureClient
- Automatic disconnect/reconnect as clients move in and out of network range
- Seamless connection experience while roaming
- Automatic and transparent upgrades, with no administrator privileges required
- Supports most existing features of SecureClient, including Office Mode, Desktop Firewall, Secure Configuration Verification (SCV), Secure Domain Login (SDL), and Proxy Detection
- Supports many additional new features, and will support even more new features in the near future
- Does not require a SmartCenter server upgrade
- Discovery and SecureClient can coexist on client systems during migration period

Note - Check Point will end its support for SecureClient in mid-2011.

Things to Consider Before Migrating to Discovery

Before migrating, you should weigh the following issues.

Note - Discovery supports VPN gateway redundancy with Multiple Entry Point (MEP) (on page 30).

Server and Client Requirements

- **Server**: Version NGX R65 HFA 60 on SecurePlatform, IPSO, and Microsoft Windows

  Note - R70 will be supported in the next release.

- **Clients**: Discovery can be installed on these platforms:
  - Microsoft Windows XP 32 bit SP2, SP3
  - Microsoft Windows Vista 32 bit and 64 bit SP1
  - Microsoft Windows 7 32 bit and 64 bit

SecureClient Features Not Yet Supported

Currently, these features of SecureClient are not supported in Discovery.

Feature	Description
Single Sign-on (SSO)	One set of credentials to log in to both VPN and Windows OS
“Suggest Connect” Mode (Auto Connect)	Initiate VPN tunnel when the client system generates traffic to the VPN domain resources
Pre/Post Connect Script	Execute manual scripts before and after VPN tunnel is established
Entrust Entelligence Support	Entrust Entelligence package providing multiple security layers, strong authentication, digital signatures, and encryption
Diagnostic Tools	Tools for viewing logs and alerts
Compression	Compress IPSec traffic
VPN Connectivity to VPN-1 VSX	Terminate VPN tunnel at Check Point VSX gateways
DNS Splitting	Support multiple DNS servers
"No Office Mode" Connect Mode	Connect to the VPN gateway without requiring Office Mode

Discovery Feature List

In This Section

SecureClient Features Supported in Discovery

Feature	Description
Authentication Methods	• Username/Password • Certificate • SecurID (passcode, softID, key fobs) • Challenge response
Cached Credentials	Cache credentials for user login
NAT-T/Visitor Mode	Allow user to connect from any place, such as a hotel, business center, and so on
Multiple Entry Point (MEP)	VPN gateway redundancy (Multiple Entry Point (MEP) "Multiple Entry Point (MEP)" on page 30)
Pre-Configured Client Packaging	Pre-package client with settings and configurations for easy provisioning to client systems
Office Mode	Internal IP address for remote access VPN users
Compliance Policy - Secure Configuration Verification (SCV)	Ensure client system security compliance before allowing remote access to internal network
Proxy Detect / Replace	Detect proxy settings in the client system web browser to allow seamless connectivity
Route All Traffic	Send all traffic from the client system through the VPN gateway
Localization	Languages supported: • Chinese (simplified) • English • French • German • Hebrew • Italian • Japanese • Russian • Spanish
Link Selection	Multiple interface support with redundancy
Certificate Enrollment / Renewal	Automatic enrollment and renewal of certificates issued by Check Point Internal CA server
CLI and API Support	Manage client by third party software or script
Tunnel Idleness	Disconnect VPN tunnel when there is no traffic for a certain length of time
Dialup	Support dialup connections
Disconnect On Smart Card Removal	Disconnect VPN tunnel when Smart Card is removed from the client system
Re-authentication	Timeout for re-authentication
Keep-alive	Send keep-alive messages from the client system to the VPN gateway to maintain the VPN tunnel

Feature	Description
Check Gateway Certificate in CRL	Validate VPN gateway certificate in the CRL list
Desktop Firewall Configured from SmartDashboard Desktop Policy	Personal firewall integrated into client, managed using the desktop policy in SmartDashboard
Configuration File Corruption Recovery	Automatically recover configuration files if they are corrupted
Secondary Connect (Including Fast Failover)	Connect to multiple VPN gateways simultaneously and establish VPN tunnels to all resources located behind each VPN gateway at the same time
Secure Domain Login (SDL)	Establish VPN tunnel prior to user login
Desktop Firewall Logs Displayed in SmartView Tracker	Desktop firewall logs are presented in SmartView Tracker
End-user Configuration Lock	Restrict user from changing the client configuration
Update Dynamic DNS with the Office Mode IP	Integrate internal IP address for remote access VPN users into Dynamic DNS
Secure Authentication API (SAA)	Integrate with third party authentication providers
SmartView Monitor	Monitor VPN tunnel and user statistics within SmartView
DHCP Automatic Lease Renewal	Automatically renew IP addresses obtained from DHCP servers

New Discovery Features

Feature	Description
Hotspot / Hotel Network Detection and Registration (Exclusion for Policy)	• Automatically detect hotspots that prevent the client system from establishing the VPN tunnel • Open a mini-browser to allow the user to register to the hotspot and connect to the VPN gateway • Firewall support for hotspots
Automatic Connectivity Detection	Automatically detect whether the client system is connected to the Internet or LAN
Automatic Certificate Renewal in CLI Mode	Support automatic certificate renewal, including in CLI mode
Location Awareness	Automatically determine if client system is inside or outside the enterprise network
Roaming	Maintain VPN tunnel as client system disconnects and reconnects using different network interfaces
Automatic and Transparent Upgrade Without Administrator Privileges	Update the client system securely and without user intervention

Feature	Description
Windows Vista / Windows 7 64 Bit Support	Support the latest 32 and 64 bit Windows OS's
Automatic Site Detection	During first time configuration, the client system detects the VPN site automatically Note: This requires DNS configuration and is only supported when configuring the client within the internal network
Geo Clusters	Connect client system to the closest VPN gateway based on location For more information on geo clusters, see white paper SK43107
Machine Idleness	Disconnect VPN tunnel when client system becomes locked
Flush DNS Cache	Remove previous DNS entries from the DNS cache when establishing VPN tunnel

Chapter 2

Configuring Security Gateways to Support Discovery

In This Chapter

Installing Hotfix on Security Gateways

If you intend to run Discovery and SecureClient simultaneously on client systems, you can install the hotfix on production gateways or on a standalone, self-managed gateway. The hotfix does not have to be installed on the SmartCenter server.

Important - If you choose to install the hotfix on production gateways, make sure that the encryption domains of these gateways **fully overlap** with the encryption domains of all other gateways, and that all gateways provide connectivity to the same resources.

SecureClient sees and tries to connect to all gateways. If the gateways on which you have installed the hotfix do not provide access to the same resources as all other gateways, client systems may have connectivity problems.

To install the hotfix on a Security Gateway:

1. Download the hotfix from the Check Point Support Center (http://supportcenter.checkpoint.com).
2. Run the hotfix:
   - On SecurePlatform:

```
[admin@gateway ~/hf]$ tar -zxvf hotfix_file.tgz

[admin@gateway ~/hf]$ ./fw1_HOTFIX_ENFI_HFA_EVE2_620631013_1

Do you want to proceed with installation of Check Point fw1 NGX R65
Support ENFI_HFA_EVE2 for Check Point VPN-1 Power/UTM NGX R65 on this
computer?

If you choose to proceed, installation will perform CPSTOP.

(y-yes, else no):y
```

   - On Windows, double-click the installation file and follow the instructions.
3. If WebUI is enabled on the gateway, it must listen on a port other than 443. Otherwise, Discovery will not be able to connect.
4. Reboot the Security Gateway.

Configuring SmartDashboard

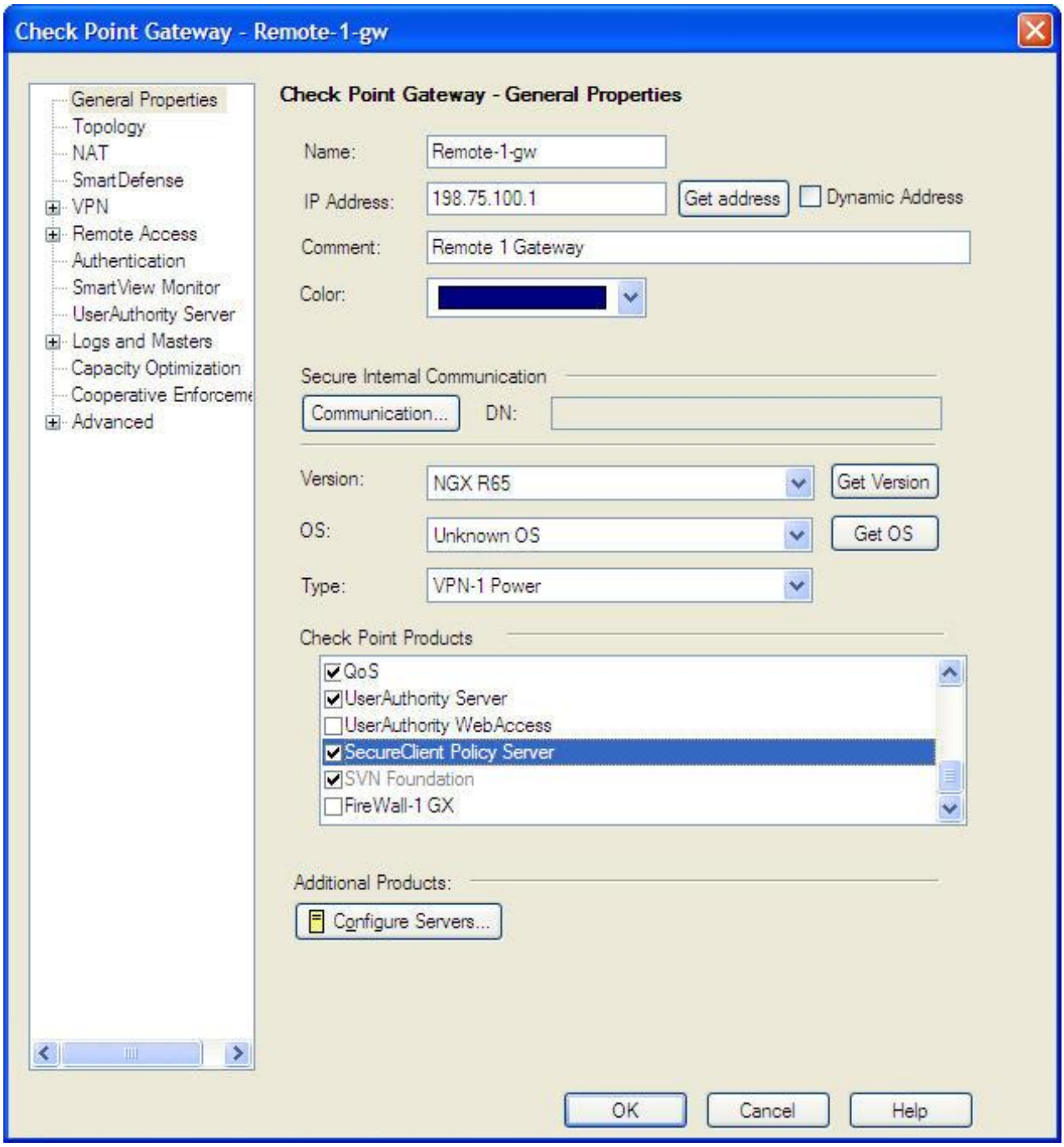
You manage Discovery through the SmartDashboard. This task explains how to set up the SmartDashboard to access Discovery configurations. Before you begin, make sure you have a network for Office Mode allocation. If you do not have such a network set up, create it now.

To configure SmartDashboard for Discovery:

1. Set the Security Gateway to be a policy server:
   a) In the Network Objects Tree, right click the Security Gateway and select **Edit**.

      The **Check Point Gateway - General Properties** window opens.

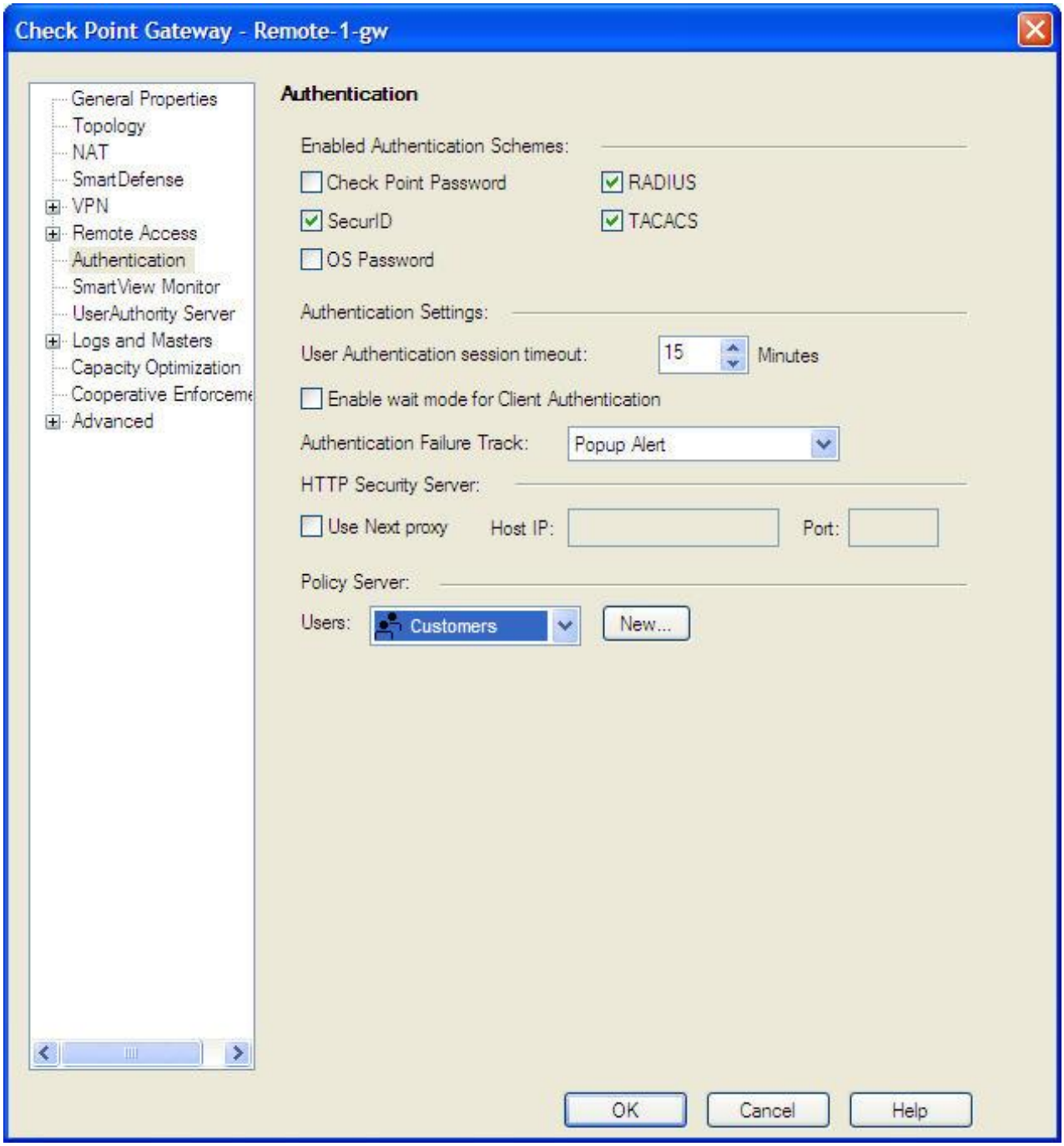
Figure 2-1 General Properties



   b) In **Check Point Products**, select **SecureClient Policy Server**.
   c) In the left navigation tree, select **Authentication**.

The **Authentication** window opens.

Figure 2-2 Authentication



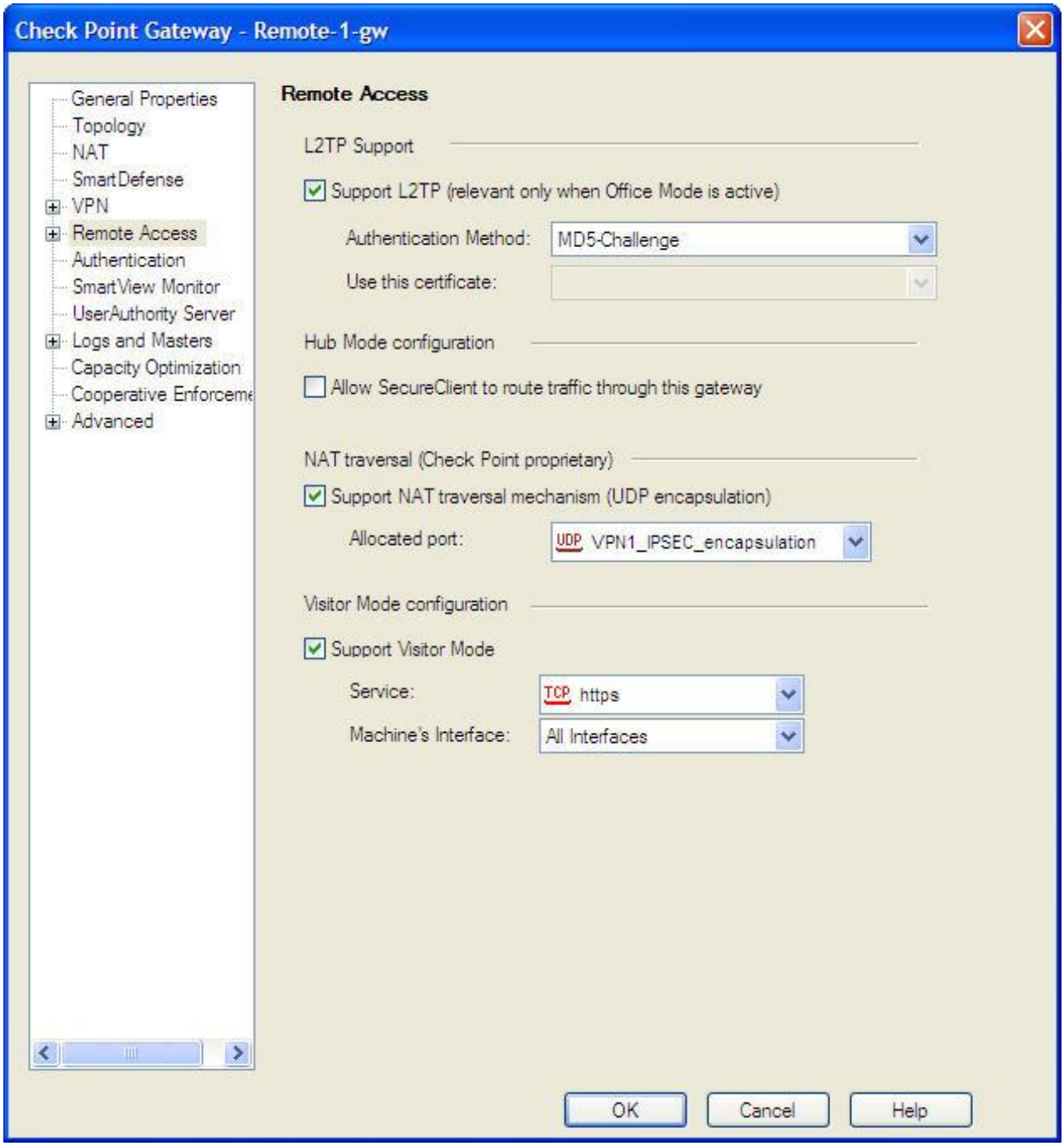
d) In **Policy Server**, select an existing user group, or create a new user group, to be assigned to the policy.

2. Configure Visitor Mode, if it is not already configured:

a) In the left navigation tree, select **Remote Access**.

The **Remote Access** window opens.

Figure 2-3 Remote Access



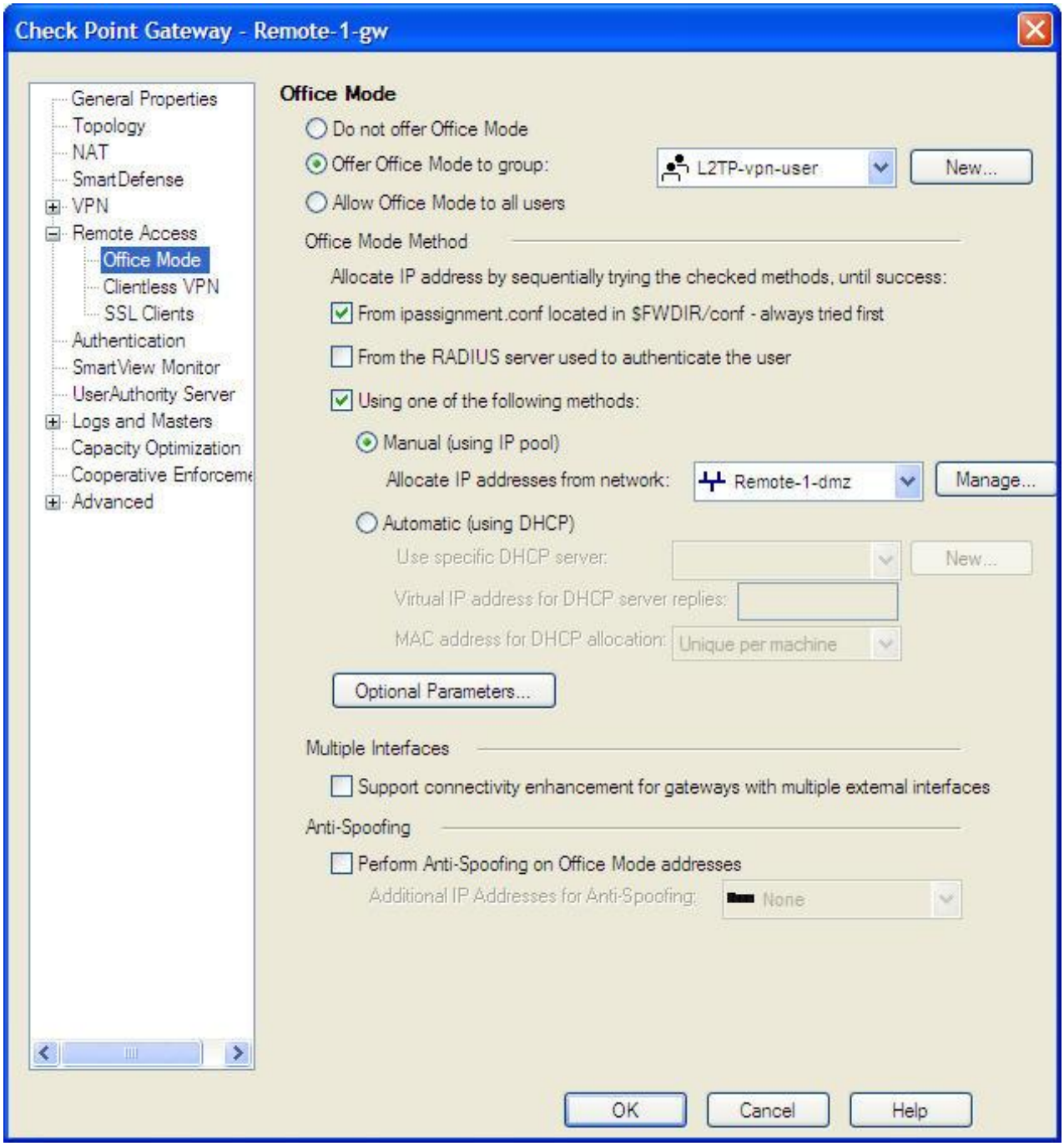
b) In **Visitor Mode configuration**, select **Support Visitor Mode**.

3. Configure Office Mode, if it is not already configured:

a) In the left navigation tree, select **Remote Access** > **Office Mode**.

The **Office Mode** window opens.

Figure 2-4 Office Mode



b) In **Office Mode Method**, select **Manual (using IP pool)**.

c) In **Allocate IP addresses from network**, select the network for Office Mode allocation.

4. Click **OK**.
5. Make sure that the Security Gateway is in the Remote Access community:

a) Select **Manage** > **VPN Communities**.

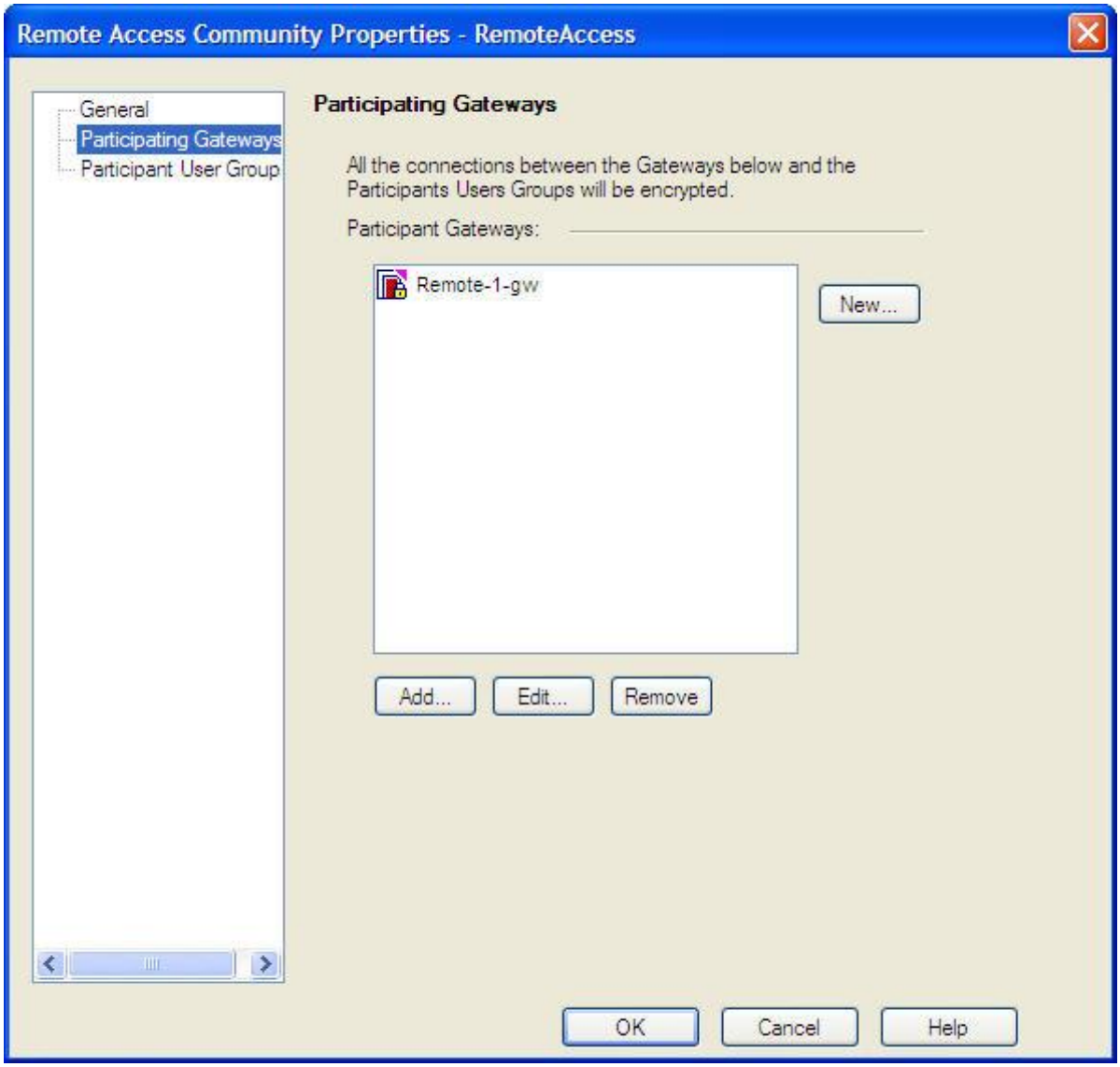
The **VPN Communities** window opens.

b) Double-click **RemoteAccess**.

The **Remote Access Community Properties** window opens.

In the left navigation tree, select **Participating Gateways**.

Figure 2-5 Participating Gateways



c) If the Security Gateway is not already in the list of participating gateways: click **Add**, select the Security Gateway from the list of gateways, and click **OK**.

d) Click **OK**.

e) Click **Close**.

6. Make sure that the desktop policy is configured correctly.
7. Install the policy.

Supporting Discovery and SecureClient Simultaneously

If you intend to run Discovery and SecureClient simultaneously on client systems, ensure that:

- The encryption domains on the gateways on which you install the hotfix fully overlap with the encryption domains of all other gateways, and that all gateways provide connectivity to the same resources (see the note in Installing Hotfix on Security Gateways (on page 9)).
- The SecureClient policy lets Discovery make outbound connections, by doing one of the following:
  - Configure desktop rules to allow outbound connections on ports TCP/443, TCP/80, and UDP/4500.

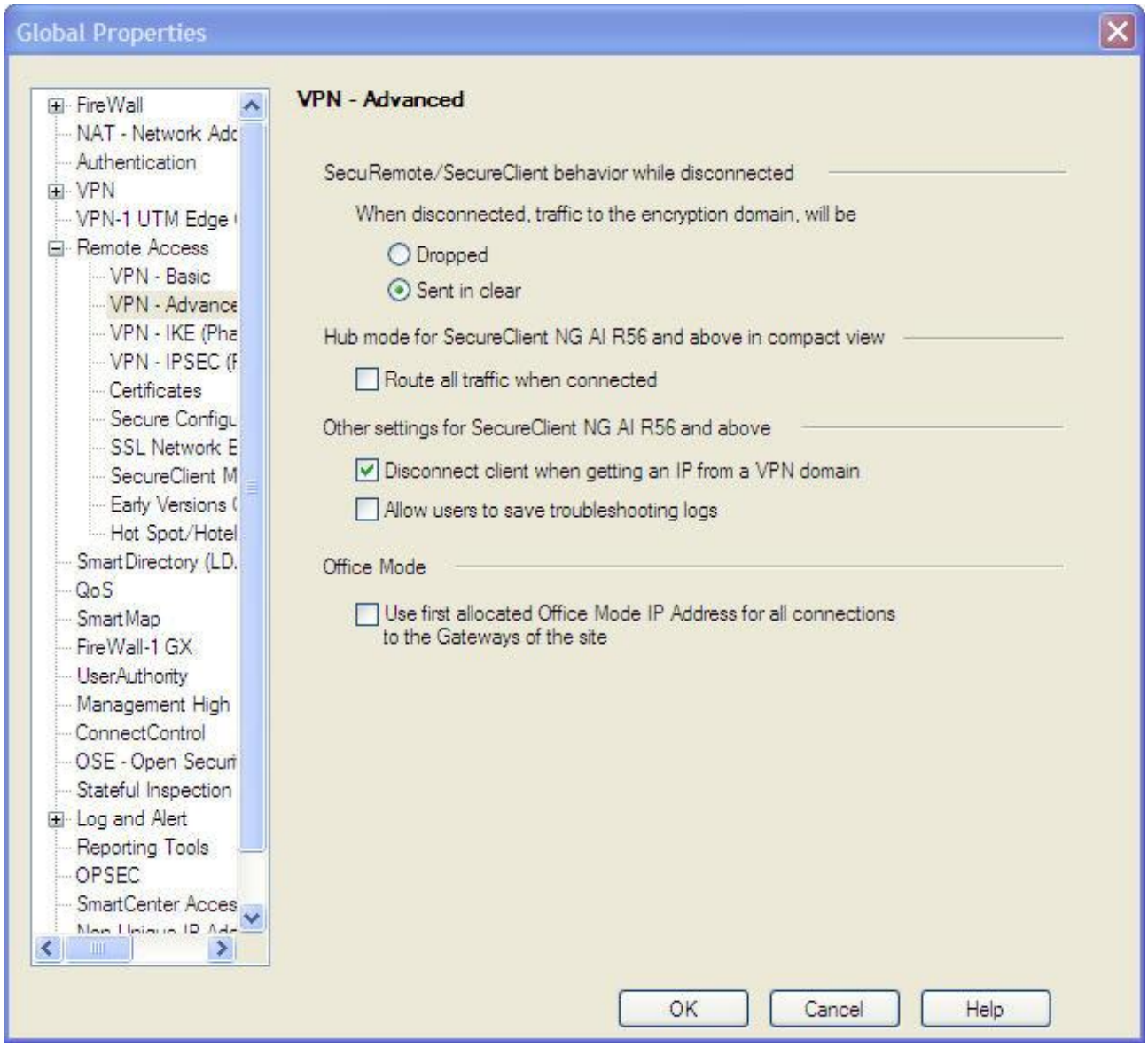
- Disable the policy on SecureClient. Note that the policy will be re-enabled when the client system reboots.
- Configure clear traffic when SecureClient is disconnected (see below).

- If secure configuration verification (SCV) is configured, add an exception for Discovery (see below).

To configure clear traffic when SecureClient is disconnected:

1. In SmartDashboard, select **Policy** > **Global Properties**.
   The **Global Properties** window opens.
2. In the left navigation tree, select **Remote Access** > **VPN - Advanced**.

Figure 2-6 VPN - Advanced



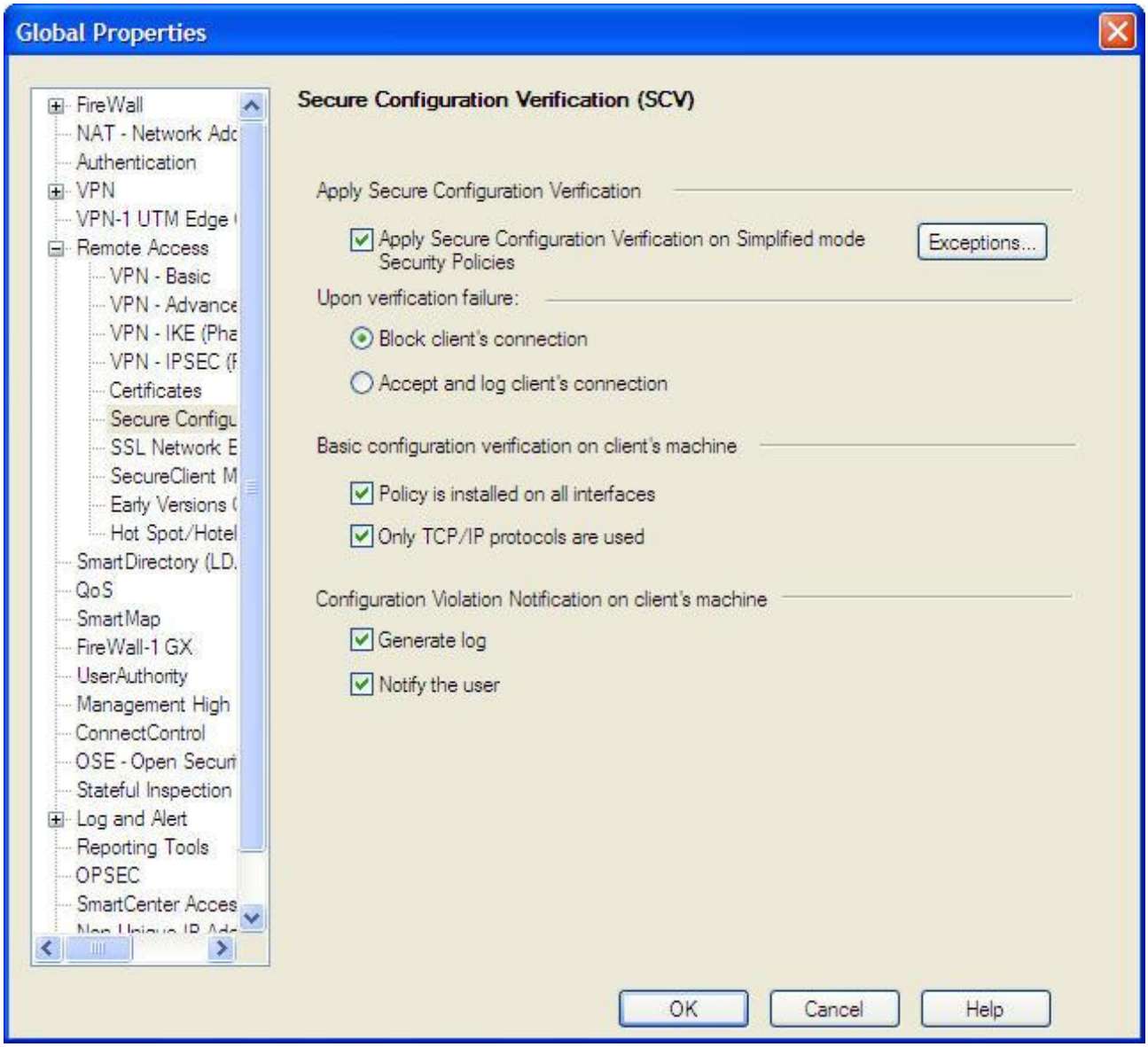
3. In **SecuRemote/SecureClient behavior while disconnected**, in the field **When disconnected, traffic to the encryption domain will be**, select **Sent in clear**.
4. Click **OK**.

To add an exception for Discovery to SCV:

1. In SmartDashboard, select **Policy** > **Global Properties**.
   The **Global Properties** window opens.

2. In the left navigation tree, select **Remote Access** > **Secure Configuration Verification (SCV)**.

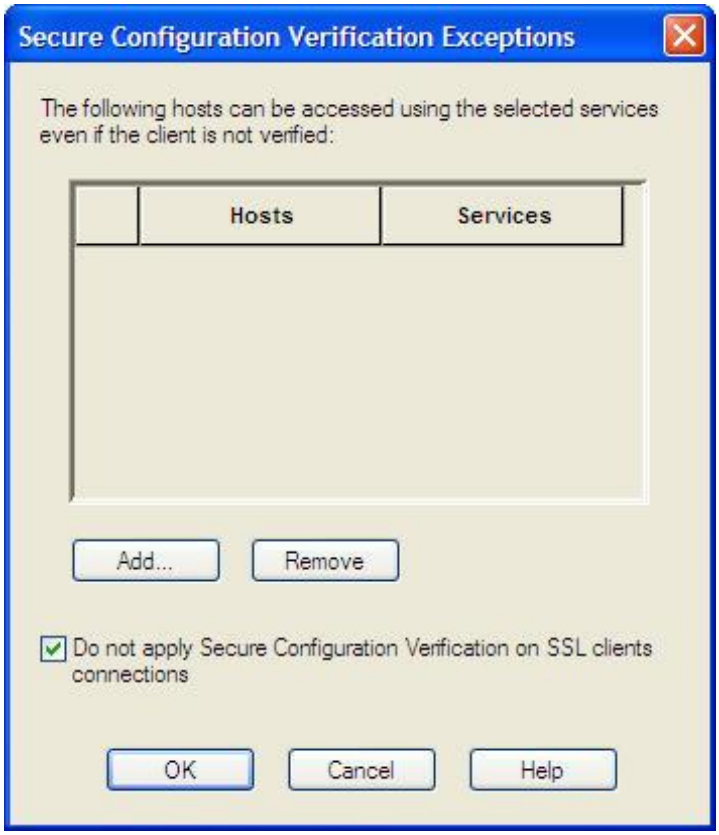
Figure 2-7 Secure Configuration Verification (SCV)



3. Select **Apply Secure Configuration Verification on Simplified mode Security Policies**.
4. Click **Exceptions**.

The **Secure Configuration Verification Exceptions** window opens.

Figure 2-8 Secure Configuration Verification Exceptions



5. Select **Do not apply Secure Configuration Verification on SSL clients connections**.
6. Click **OK**.
7. Click **OK**.

Installing and Configuring Discovery on Client Systems

Installing Discovery on Client Systems

The Discovery installation package is a single self-installing executable that you can download from the Check Point Download Center.

Understanding the Tray Options

After installing Discovery, the client icon  appears in the system tray. This icon changes, depending on the client's status:

Icon	Status
	Disconnected
	Connecting
	Connected
	Encryption (encrypted data is being sent or received on the VPN)
	Error

You can also hover your mouse over the icon to display the client's status.

Right-click the icon to open the system tray options menu. Note that only some of these options may appear, depending on the client's status and depending on how your client is configured.

Option	Function
Connect	Open the main connection window with the last active site selected. If you authenticate using a certificate, the client immediately attempts to connect using the selected site.
Connect to	Open the main connection window.
VPN Options	Open an options window for site and advanced settings.
Give us your feedback	Open a window in your browser to provide feedback to Check Point.
Enable/Disable Security Policy	Enable/Disable the security policy provided by the Security Gateway. This option is usually not available.
Help > About	Display information about the client, including version number.
Help > Help Contents	Open the help file.
Help > Collect Logs	Archive the logs. When finished, the archive is automatically opened.
Show Client	Display information about the client.

Option	Function
Shutdown Client	Close Discovery. Any open VPN tunnel is closed. However, a background service continues to run, and will respond to CLI commands. To stop this service, enter at a command line: `net stop tracsrvwrapper`

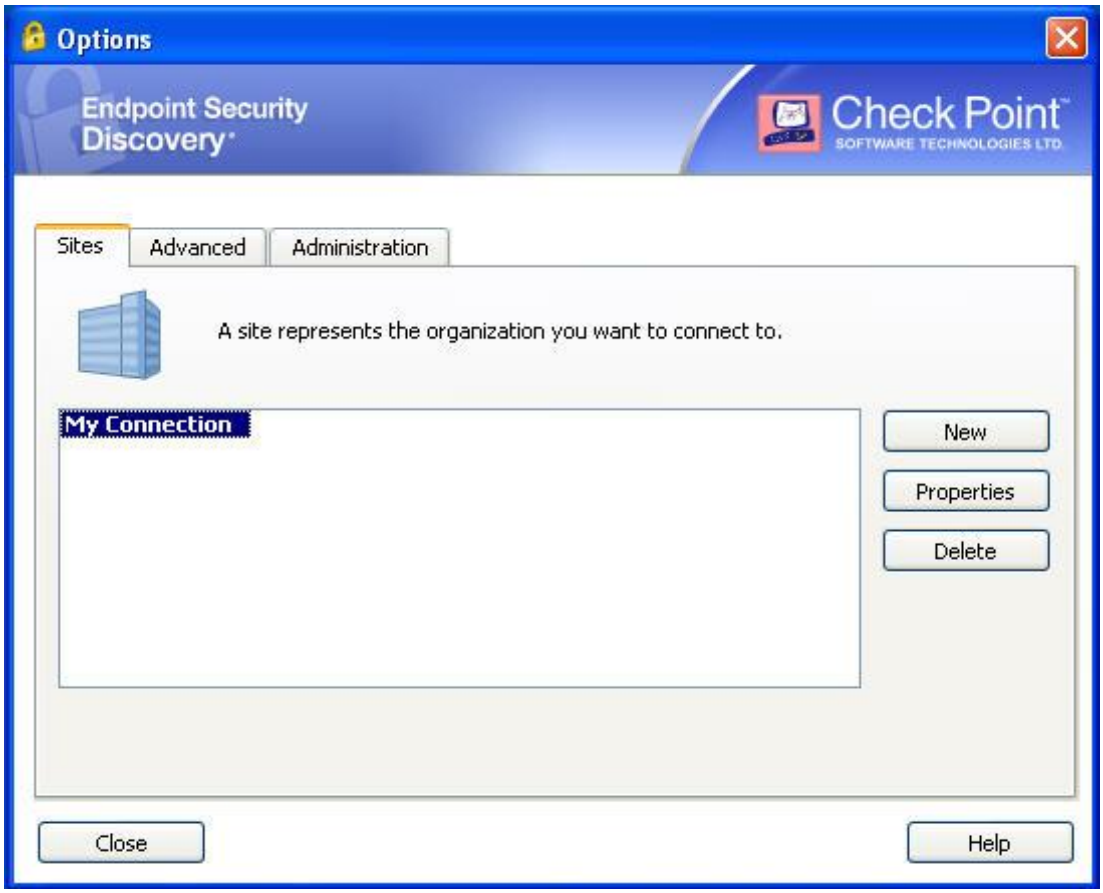
Configuring Discovery

Creating a Site

To create a site:

1. Right-click the client icon and select **VPN Options**.
   The **Options** window opens. The first time you open this window, no sites will be listed.

Figure 2-9 Discovery Options: Sites



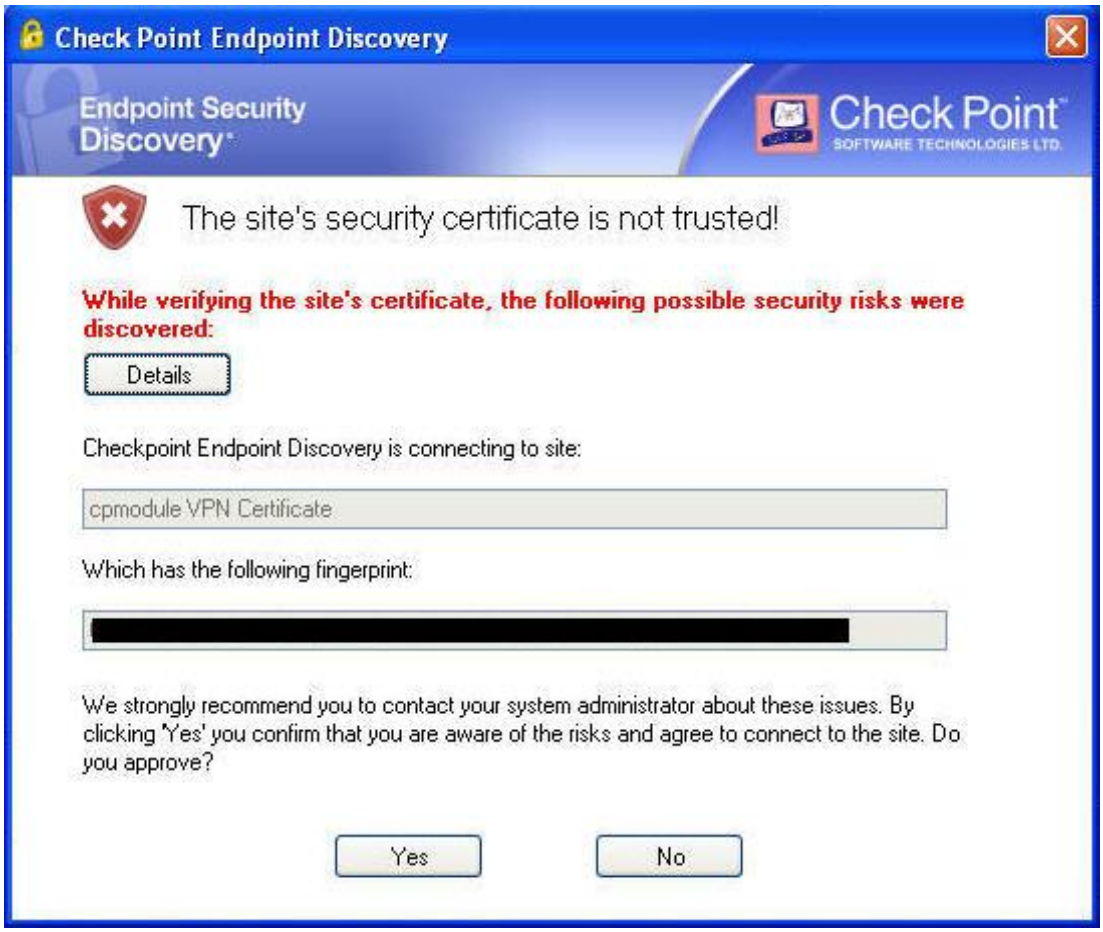
2. On the **Sites** tab, click **New**.
   The Site Wizard starts.

3. Click **Next**.

Figure 2-10 Site Wizard: Enter Server Address

4. Enter the name or IP address of the Security Gateway, and an optional display name, and click **Next**.
   The site name is resolved, which may take a few minutes.
   After resolving the site, a security warning window may open.

Figure 2-11 Site Wizard: Warning



If a security warning window opens:

a) Verify that the site's fingerprint is correct.

b) Click **Details** to see any further warnings.

c) If the site's details are correct, click **Yes** to continue. The fingerprint is stored in the Windows registry and the security warning is not opened again for this site, even if the client is upgraded.

Otherwise, click **No** and check the fingerprint and other settings on the Security Gateway.

If you did not receive, or you have resolved, a security warning, the **Authentication Method** window opens.

Figure 2-12 Site Wizard: Authentication Method

5. Select an authentication method, and click **Next**.
   - If you selected **Certificate**, complete the information, and click **Next**.
   - If you selected **SecurID**, select the type, and click **Next**.
6. Click **Finish** to close the Site Wizard.

   The client offers to connect you to the newly-created site.
7. Click **Yes** to connect to the site, or **No** to cancel.

Connecting to a Site

To connect to a site:

1. Right-click the client icon and select **Connect** or **Connect to**.

A site connection window opens.

Figure 2-13 Site Connection

2. If you selected **Connect to**, you can select the site to which you would like to connect.
3. Enter your authentication credentials, and click **Connect**.
   A connection progress window opens.

Figure 2-14 Connection Progress

If you entered the correct credentials, the client runs security compliance verification (SCV) to determine whether the client system is secured by such things as antivirus software, the presence of a firewall, recommended and relevant software updates, and so on.

- If the client system fails SCV, the client displays a report that contains links to online remediation sources. Follow the links to correct the problems discovered by SCV, and then try to connect again.
- If the client passes SCV, the client is now connected.

Configuring Proxy Settings

Note - In most cases, the remote location's proxy server settings are detected automatically.

To configure proxy settings:

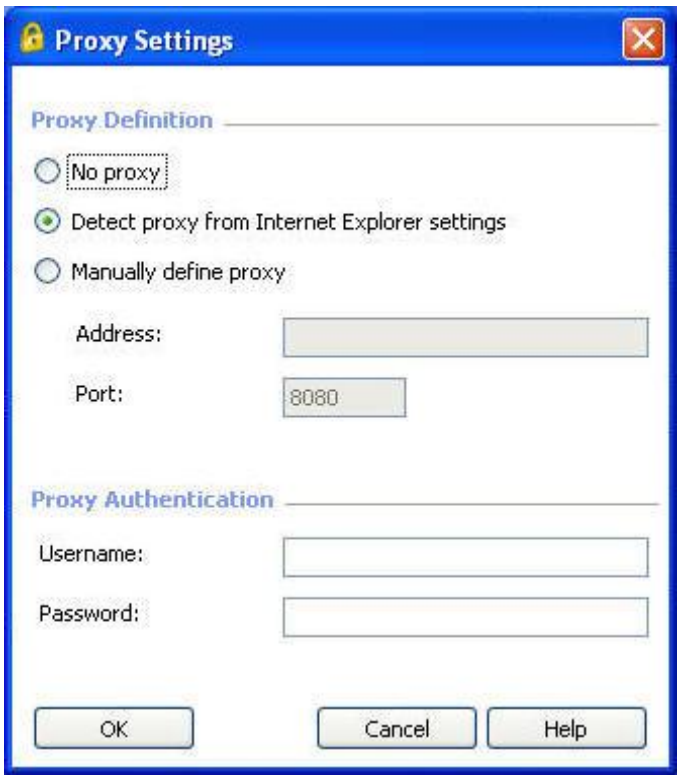
1. Right-click the client icon and select **VPN Options**.
   The **Options** window opens.

2. Click the **Advanced** tab.

Figure 2-15 Discovery Options: Advanced

3. Click **Proxy Settings**.
   The **Proxy Settings** window opens.

Figure 2-16 Discovery Options: Proxy Settings



4. Select one of the following:
   - **No proxy**

- **Detect proxy from Internet Explorer settings**

  If you select this option, the settings in Internet Explorer must be manually defined. In Internet Explorer under **Tools > Internet options > Connections > LAN Settings**, verify that **Use a proxy server for your LAN** is selected, and that the correct IP address and port number are entered.

  If either **Automatically detect settings** or **Use automatic configuration script** is selected, Discovery cannot detect the proxy settings from Internet Explorer.

- **Manually define proxy**

  Enter the IP address and port number of the proxy.

5. If you selected to use a proxy, enter a valid user name and password for the proxy.
6. Click **OK** to save your changes.

Configuring VPN Tunneling

For the Security Gateway to act as a hub for content inspection of all inbound and outbound client traffic, regardless of destination, the Security Gateway administrator must define a network application that includes the range: **0.0.0.1 > 255.255.255.254**.

To configure VPN Tunneling:

1. Right-click the client icon and select **VPN Options**.
   The **Options** window opens.
2. On the **Sites** tab, select the site to which you wish to remain connected, and click **Properties**.
   The **Properties** window for the site opens.
3. Select the **Settings** tab.

Figure 2-17 Discovery Site Properties

4. In **VPN tunneling**, click **Encrypt all traffic and route to gateway**.
5. Click **OK**.

Using the Packaging Tool

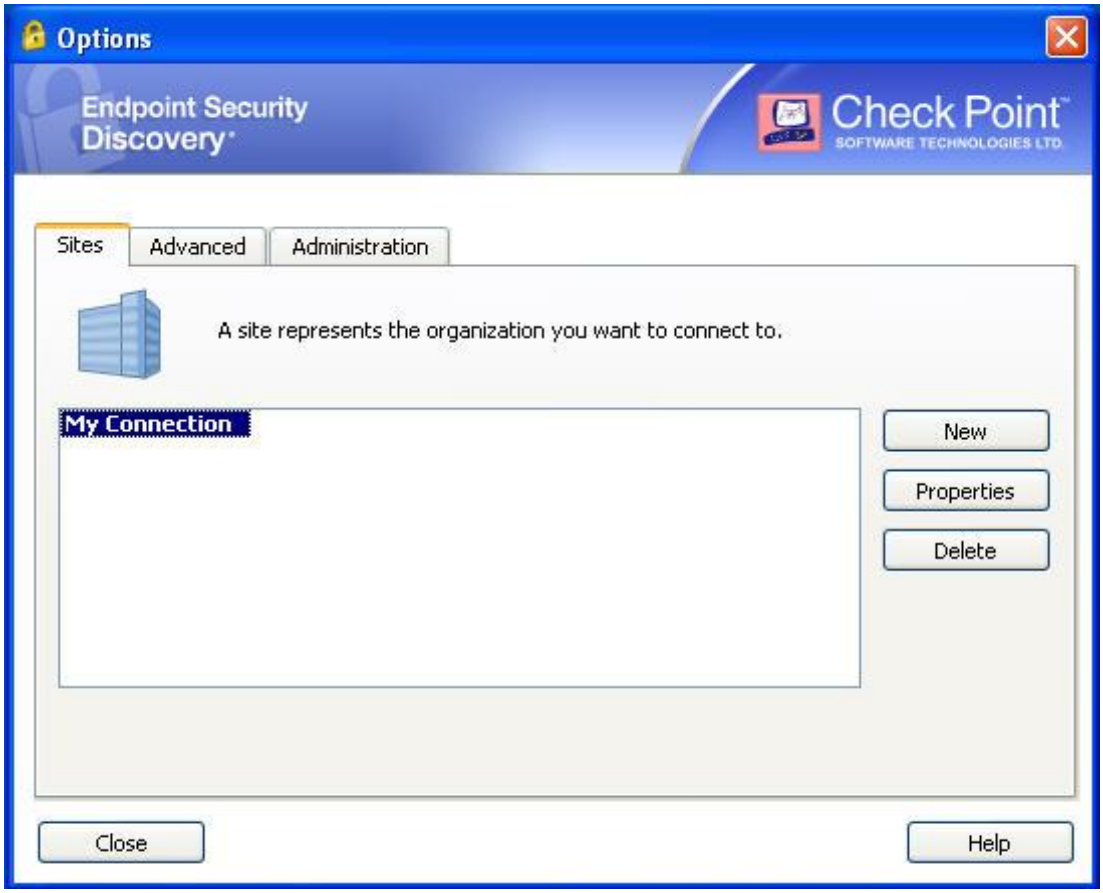
If you plan to distribute Discovery to many client systems, you can save time by creating a preconfigured installation package.

A preconfigured installation package is also more suitable for users if they will install Discovery on their own systems.

To create a preconfigured package:

1. Run **c:\Program Files\Checkpoint\Endpoint Connect\AdminMode.bat** on the client system.
   Discovery restarts in administration mode.
2. Right-click Discovery in the system tray, and select **VPN Options**.
   The **Options** window opens.

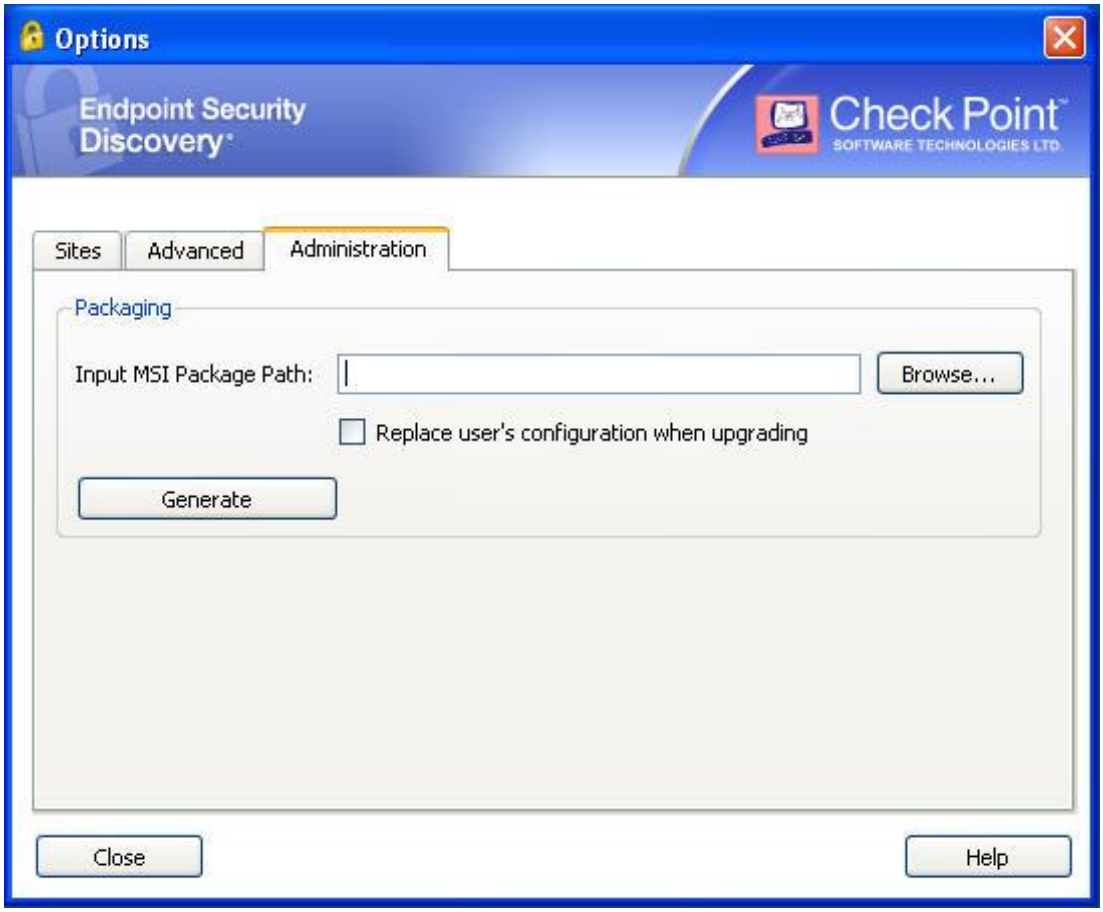
Figure 2-18 Discovery Options: Sites



3. Configure the client as required.

4. Select the **Administration** tab.

Figure 2-19 Discovery Options: Administration



5. In **Input MSI Package Path**, enter or select a directory to which to save the preconfigured package.
6. To cause the package to override user configurations on the client systems, select **Replace user's configuration when upgrading**.
7. Click **Generate** to create the preconfigured installation package.

Distribute this preconfigured installation package to the client systems.

The Configuration File

Configuration parameters are passed from the Security Gateways to the client system using a configuration file. The configuration file is located on the Security Gateway in **$FWDIR/conf/trac_client_1.ttm**. The file is a text file and can be edited using any text editor, such as Notepad.

After editing the file, install the policy.

Note - When editing the configuration file, do not use an advanced word processor, such as Microsoft Word, which may add formatting codes to the file.

Centrally Managing the Configuration File

If the configuration file on each client system is identical, you can manage a single copy of the configuration file on the SmartCenter server, which will be copied to the Security Gateways when you install the policy. To do this, you must edit a file on the SmartCenter server.

To centrally manage the configuration file:

Add the following line to **$FWDIR/conf/fwrl.conf**:

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

Key Parameters in the Configuration File

The following table lists certain important parameters that are set in the configuration table.

The default value is the recommended value. Where the default value is listed as "none", there is no default value, or the default value is empty.

Parameter	Description	Default
allow_disable_firewall	Enable/disable menu option allowing user to disable desktop firewall	false
certificate_key_length certificate_strong_protection certificate_provider internal_ca_site internal_ca_dn	Certificate enrollment settings	1024 true "Microsoft Enhanced Cryptographic Provider v1.0" none none
connect_timeout	Time, in seconds, after which Discovery gives up trying to connect	70000
default_authentication_method	Default authentication for a new site	none
disconnect_on_smartcard_removal	Enable/disable client disconnection when smart card containing current certificate is removed	false
do_proxy_replacement	Enable/disable proxy replacement	true
enable_capi	Enable/disable CAPI authentication	true
enable_gw_resolving	Enable/disable DNS resolution on each connection Used for MEP	true

Parameter	Description	Default
flush_dns_cache	Enable/disable flushing the DNS cache when starting up	false
hotspot_detection_enabled	Enable/disable automatic hotspot detection	true
ips_of_gws_in_mep	List of Security Gateway IP addresses to which the client should attempt to connect Addresses are separated by "&#", and the list is terminated by a final "&#", as follows: `NNN.NNN.NNN.NNN&#MMM.MMM.MMM.MMM&#`	none
mep_mode	MEP mode, indicating how to use the list of Security Gateways defined in ips_of_gws_in_mep One of: • dns_based • first_to_respond • primary_backup • load_sharing	dns_based
predefined_sites_only	Enable/disable user ability to create or modify sites	false
send_client_logs	A list of email addresses to which debug logs are sent	none
suspend_tunnel_while_locked	Enable/disable suspending traffic when client is locked	false
tunnel_idleness_ignore_icmp	Enable/disable monitoring ICMP packets to determine if a tunnel is active	true
tunnel_idleness_ignored_tcp_ports	A list of TCP ports that are not monitored to determine if a tunnel is active	none
tunnel_idleness_ignored_udp_ports	A list of UDP ports that are not monitored to determine if a tunnel is active	53&#137&#138&#
tunnel_idleness_timeout	Time, in seconds, after which a client will close an inactive tunnel	0

Appendix A

Multiple Entry Point (MEP)

In SecureClient, Security Gateways were required to belong to the same VPN to use MEP. In Discovery, Security Gateways are not required to belong to the same VPN and the client does not send probing RDP packets to discover available Security Gateways.

To enable MEP:

1. In the configuration file:
   - Ensure that **enable_gw_resolving** is `true`.
   - Add **mep_mode**, using one of the available values:
     - **dns_based**: The client resolves Security Gateway addresses using DNS geo clustering.
     - **first_to_respond**: The client probes all Security Gateways on the list and builds a new list according to response time. The first Security Gateway to respond becomes the first Security Gateway on the list, and so on.
     - **primary_backup**: The client works sequentially through the list, attempting to connect to each Security Gateway in turn.
     - **load_sharing**: The client randomly tries Security Gateways on the list until a connection is established.
   - Add **ips_of_gws_in_mep**, using the list of available Security Gateway IP addresses.
2. Ensure that the configuration file is centrally managed (see Centrally Managing the Configuration File (on page 28)).
3. Install the policy.

Differences Between SecureClient and Discovery CLI

The following table lists common tasks and how to perform them using the CLI of SecureClient or Discovery. N/A indicates that the task cannot be performed by the CLI, either because the functionality does not exist or because the task is not relevant for the indicated client.

Task	SecureClient	Discovery
Asynchronous Connect	connectwait <profilename>	N/A
Change P12 Certificate Password	N/A	change_p12_pwd -f <filename> [-o <oldpassword> -n <newpassword>]
Connect to Site	connect [-p] <profilename>	connect -s <sitename> [-u <username> -p <password> | -d <dn> | -f <p12> | -pin <PIN> -sn <serial>]
Create / Add Site	add <sitename>	create -s <sitename> [-a <authentication method>]
Delete Site	delete <sitename>	delete -s <sitename>
Disconnect from Site	disconnect	disconnect
Display Connection Status	status	N/A

Task	SecureClient	Discovery
Enable / Disable Hotspot Registration	sethotspotreg <on | off>	N/A
Enable / Disable Policy	setpolicy [on | off]	N/A
Enroll ICA CAPI Certificate	icacertenroll <site IP/name> <registration key> <file path> <password>	enroll_capi -s <sitename> -r <registrationkey> [-i <providerindex> -l <keylength> -sp <strongkeyprotection>]
Enroll ICA P12 Certificate	N/A	enroll_p12 -s <sitename> -f <filename> -p <password> -r <registrationkey> [-l <keylength>]
Get Site Name / IP	getsite <profilename>	info [-s <sitename>]
List Profiles	listprofiles	N/A
List Domain Names Stored in the CAPI	N/A	list
Print Log Messages	N/A	log
Renew CAPI Certificate	N/A	renew_capi -s <sitename> -d <dn> [-l <keylength> -sp <strongkeyprotection>]
Renew P12 Certificate	N/A	renew_p12 -s <sitename> -f <filename> -p <password> [-l <keylength>]
Restart VPN Services	restartsc	N/A
Set Certificate File / Password	passcert <password> <certificate>	See Connect to Site
Set Username / Password	userpass <username> <password>	See Connect to Site
Show Number of Profiles	numprofiles	N/A
Show VPN Client Version	version	ver
Start VPN Client Services	startsc	start
Stop VPN Client Services	stopsc	stop
Suppress UI Dialog Messages	suppressdialogs [on | off]	N/A
Unset User Credentials	erasecreds	N/A
Update Topology	update <profilename>	N/A