Entrust® Securing Digital Identities & Information

Securing Your Digital Life

Entrust IdentityGuard 7.2 with Check Point NGX (R60), Check Point NG with Application Intelligence (R55) and Connectra NGX

OPSEC CERTIFIED

December 2005

The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Table of Contents

Introduction

This integration guide documents the integration between Check Point NG with Application Intelligence (R55), Check Point NGX (R60), Connectra NGX and Entrust IdentityGuard 7.2. The aim of this integration is to allow strong, 2-factor authentication to the Check Point IPSEC and SSL VPN solutions using Entrust IdentityGuard.

The integration of Entrust IdentityGuard and a Check Point solution requires a RADIUS server that supports challenge-response, an integral part of the RADIUS standard. To illustrate this integration, the Funk Steel Belted RADIUS Server was used to illustrate how to configure a RADIUS server with the Check Point gateways; deploying organizations can choose to leverage any RADIUS server that supports the RADIUS challenge response message.

This integration works for both the entry of Entrust IdentityGuard grid values, as well as temporary PINs.

Prerequisites

This guide does not include instructions on the installation and configuration of the individual products used. It focuses on the configuration of the products to integrate them. Please see individual product documentation for full installation and configuration instructions.

Before you start

- Install and configure the RADIUS server, using the instructions provided by the vendor
- Install and configure the Check Point solution, using the instructions provided by Check Point.

In the steps that follow you will be using the Check Point administration console and the RADIUS server to integrate Entrust IdentityGuard with your primary authentication method. Steps are outlined for integration with 2 different versions of the Check Point VPN-1/FireWall-1 product (R55 and R60) as well as with the web security gateway solution Connectra (which provides sslvpn access).

Configuration includes:

- Configuring the RADIUS server
- Configuring Check Point NG with Application Intelligence (R55)
- Configuring Check Point NGX (R60)
- Configuring Connectra NGX
- Configuring the Entrust IdentityGuard v7.2 server

Note: The following steps can be performed before or after you install Entrust IdentityGuard 7.2. In either case, ensure that you note the shared secrets, IP address and port values you use, because you will be using them here and in the installation procedure documented in the *Entrust IdentityGuard 7.2 Installation and Configuration Guide*.

Configuring the Entrust IdentityGuard server

Install the Entrust IdentityGuard 7.2 server. (See the *Entrust IdentityGuard 7.2 Installation and Configuration Guide*.)

During Entrust IdentityGuard installation, you will enter the shared secrets, IP addresses and ports you provided when you configured the Check Point NG server and the RADIUS server.

General RADIUS Configuration Overview

As stated, this integration guide documents how to use the combination of Check Point NG VPN server and the Funk Steel Belted Radius Server with Entrust IdentityGuard. If you are using another RADIUS server, the steps are similar and can be quickly understood by reading the steps below as well as the Funk Steel Belted Radius Server example.

If your remote access gateway (IP-SEC or SSL) is configured to use an existing RADIUS server for configuration, the Entrust IdentityGuard proxy service can be used to add Entrust IdentityGuard as a second factor of authentication. The proxy service works by sending the authentication request to the existing RADIUS server to perform primary authentication and then adding an Entrust IdentityGuard authentication step. Users that do not exist in Entrust IdentityGuard are authenticated by the primary authentication mechanism only.

How the Entrust IdentityGuard Proxy Service for RADIUS manages authentication

1. The VPN server sends the RADIUS authentication request to the Entrust IdentityGuard proxy service.
2. The Entrust IdentityGuard proxy service forwards the request to an existing RADIUS server.
3. The RADIUS server sends an “accept” or “reject” message to the Entrust IdentityGuard proxy service. A “reject” message is returned by the Entrust IdentityGuard proxy service to the VPN server. An “accept” message is held by the Entrust IdentityGuard proxy service.
4. If the Entrust IdentityGuard proxy service received an “accept” message from the RADIUS server, it requests an Entrust IdentityGuard challenge and sends this challenge via an “access-challenge” message to the VPN server. The challenge requires a grid coordinate response from the user’s card or a Temporary PIN response from the user (if one has been issued). Either response will work.
5. The VPN server sends the user’s response to the Entrust IdentityGuard proxy service. The Entrust IdentityGuard proxy service forwards the response to the Entrust IdentityGuard server, where it is validated.
6. If a valid IdentityGuard response, Entrust IdentityGuard sends an “accept” message to the VPN server and a tunnel is created for the user. If the response is invalid, a “reject” message is sent to the VPN server and the tunnel does not get established.

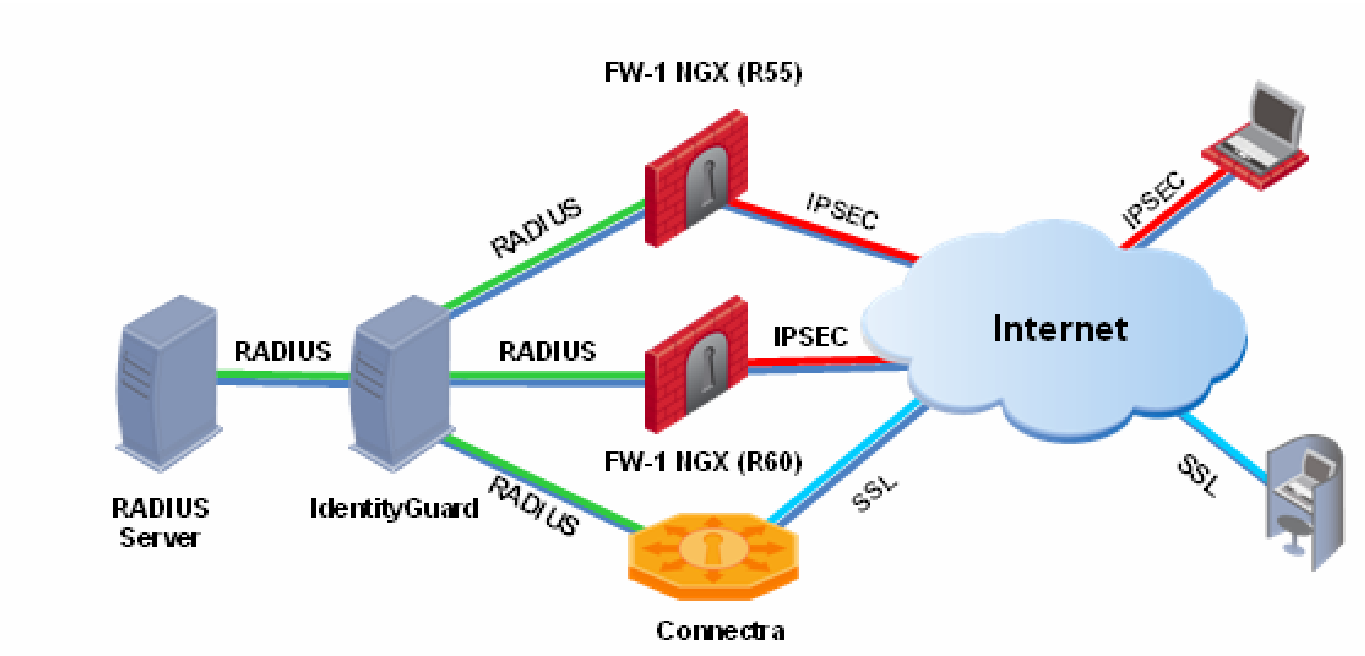
For more information, see RFC 2865 “Remote Authentication Dial in User Service (RADIUS)”, which defines the RADIUS protocol.

Integration Details

As prescribed, the following products should be installed and configured:

- **RADIUS Server:** – For this integration, Funk Steel Belted Radius Server was used. The Funk Steel Belted RADIUS server should be installed and configured with network access to the Entrust IdentityGuard server. Appropriate ports (e.g. 1812 or 1645) should be open for communication to and from the Funk Steel Belted Radius Server.
- **Check Point NG with Application Intelligence (R55 or NGX) -** The Check Point NG VPN server should be installed, configured and operational. Network connectivity should also be configured with RADIUS based communication being allowed between the Check Point NG and both the Entrust IdentityGuard and Funk SBR server.
- **Check Point Connectra NGX –** The Check Point web security gateway should be installed, configured and operational. Network connectivity should also be configured with RADIUS based communication being allowed between the Check Point Connectra gateway, the Entrust IdentityGuard and Funk SBR Server.
- **Entrust IdentityGuard Server –** The Entrust IdentityGuard and the Entrust IdentityGuard proxy server with the addresses of the Check Point NG application, the RADIUS Server and the shared secret.

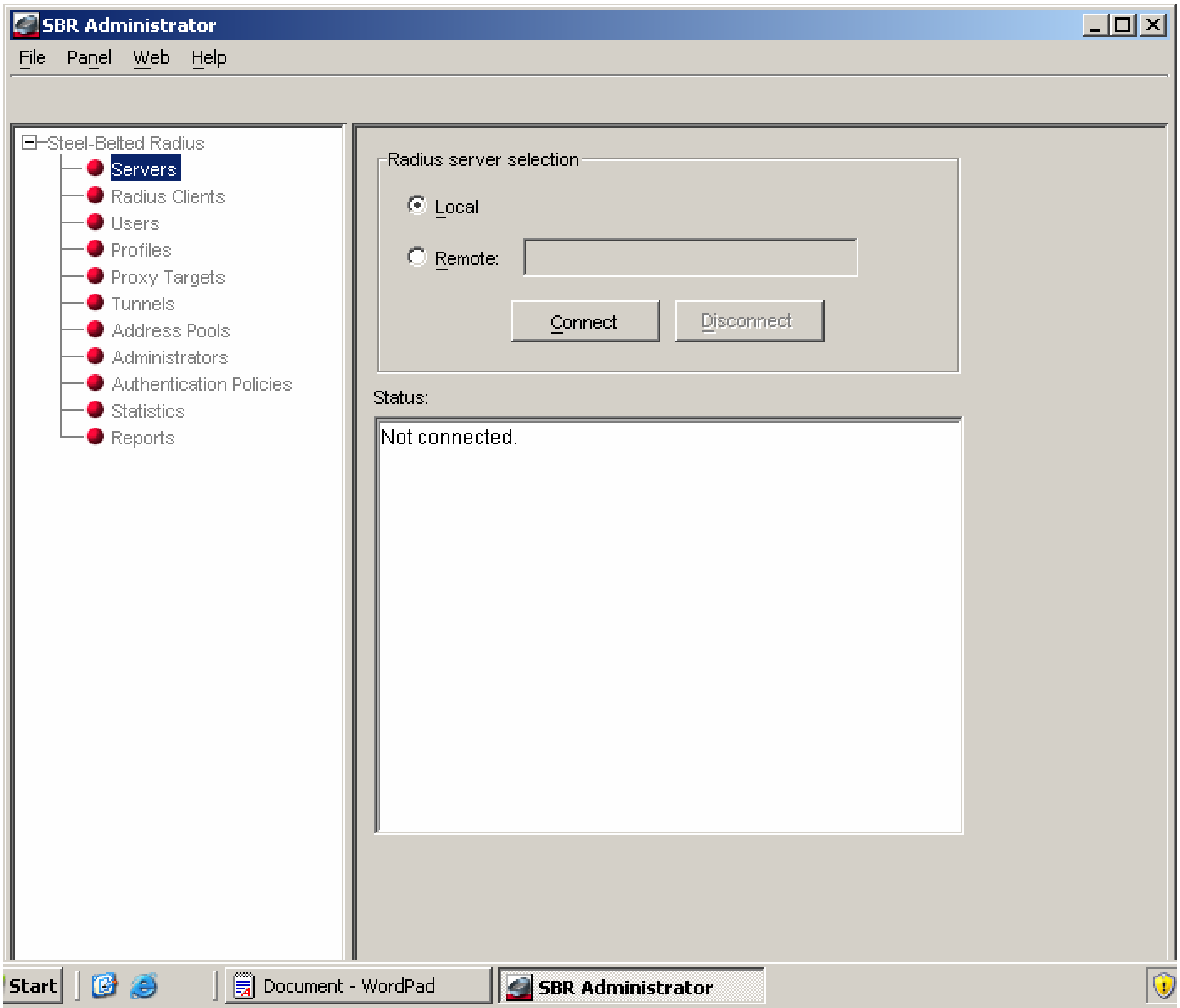
The configuration of the integrated solution is illustrated below:



Note: User IDs for end users were provisioned in both RADIUS & Entrust IdentityGuard. The user IDs must be the same in the two systems.

Configuring the RADIUS server

1. Log in to the Funk Steel Belted Radius (SBR) Server as an administrator. In the SBR Administrator Console, click the **Connect** button and enter in your username and password to authenticate.



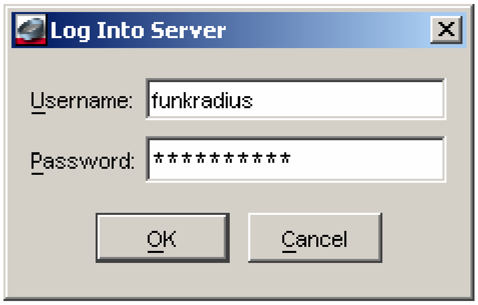
Radius server selection

● Local

○ Remote:

Status:

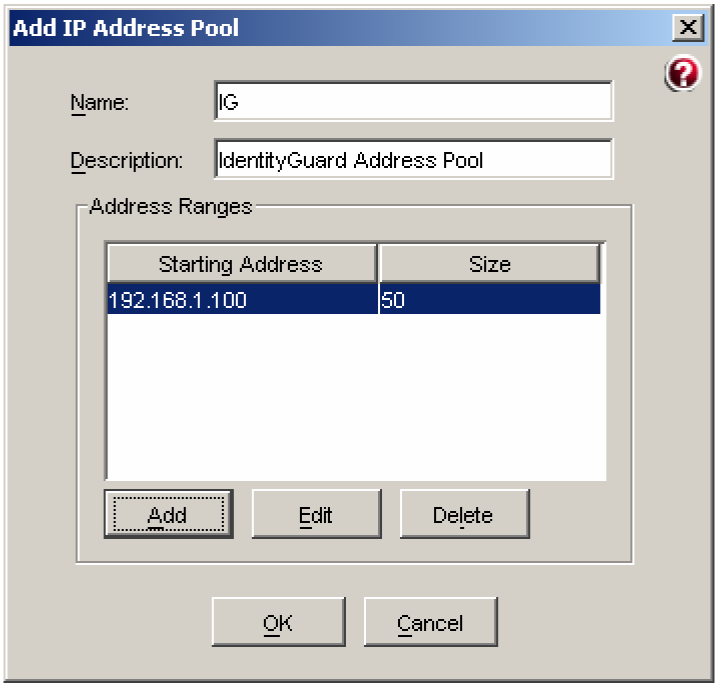
Not connected.



Username: funkradius

Password: **********

2. Before defining a RADIUS Client, we need to add an Address Pool for client connections. Click the **Address Pools** option within the left panel of the SBR Administrator console. Enter in a **Name** and **Description** for the Address Pool.



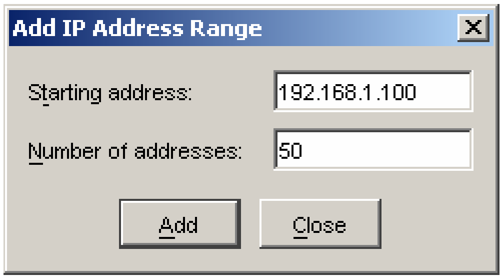
Name: IG

Description: IdentityGuard Address Pool

Address Ranges

Starting Address	Size
192.168.1.100	50

Next, Click the **Add** button and enter in the **Starting address** and **Number of addresses**. Click the OK button to save and exit.



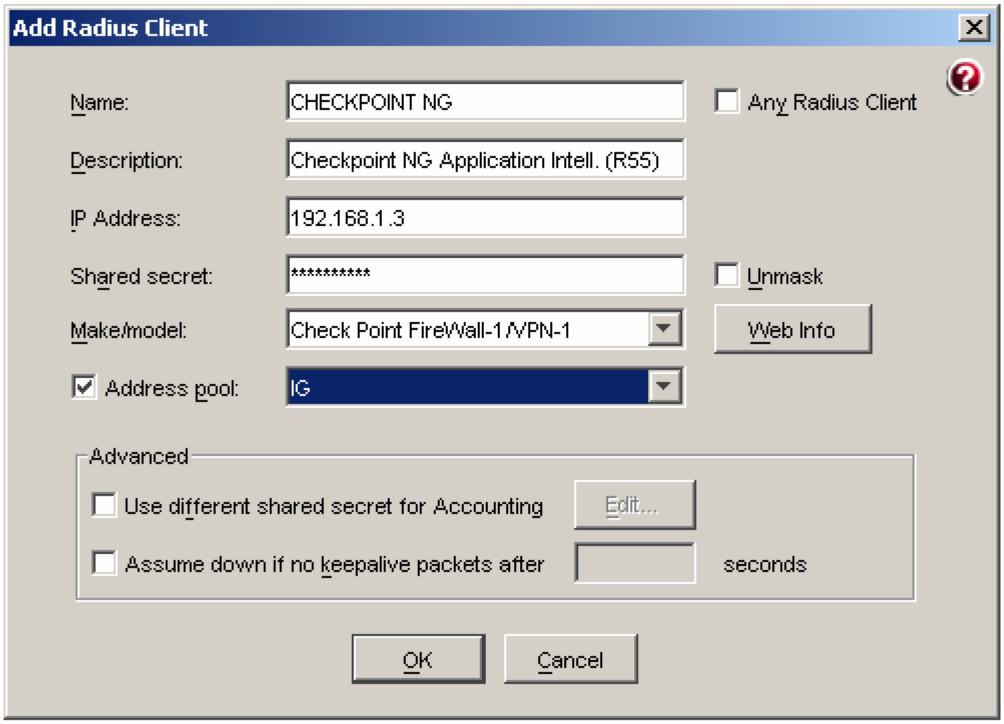
Starting address: 192.168.1.100

Number of addresses: 50

3. Next, add the Entrust IdentityGuard server as the RADIUS Client. Within the SBR Administrator Console, select the **RADIUS Clients** option button within the left pane. Then, click the **Add** button on the toolbar above.

   Enter in the details that describe your Check Point configuration.

   > **Name** – The name of the RADIUS client, such as the device's hostname, IP address, or other identifier. The RADIUS client name is used to match the NAS-Identifier attribute of RADIUS requests.
   >
   > **Description** - Optional description of the RADIUS client.
   >
   > **IP Address** – DNS hostname or IP address of the RADIUS client in IPv4 or IPv6 format. If you enter a hostname, SBR Administrator resolves the hostname to an IP address and displays the IP address for the RADIUS client.
   >
   > **Shared secret** - The authentication shared secret, which is used to verify communication between RADIUS devices.
   >
   > **Make/model** - Identifies the type of RADIUS client. The make/model you select determines the set of attributes required for users. Select Check Point FireWall-1 with this configuration.
   >
   > **Address pool** – Check this box to choose an IP address pool for the RADIUS client.
   >
   > (Note: the Name and Description below can easily be changed to reflect R60 or Connectra NGX – In either case the RADIUS client configured here is communicating with the IdentityGuard server and not directly with Check Point)



Add Radius Client

Name: CHECKPOINT NG

□ Any Radius Client

Description: Checkpoint NG Application Intell. (R55)

IP Address: 192.168.1.3

Shared secret: **********

□ Unmask

Make/model: Check Point FireWall-1/VPN-1

☑ Address pool: IG

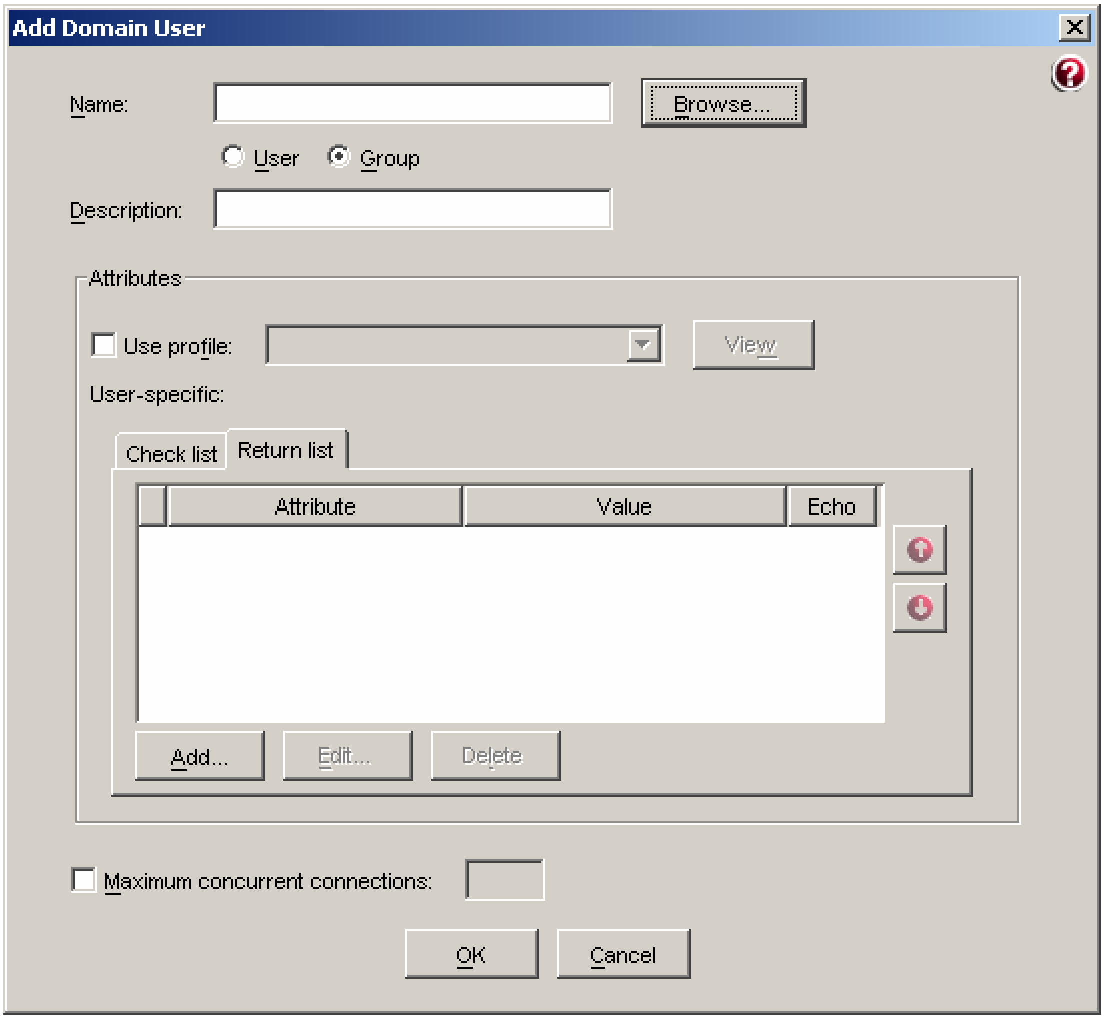
Advanced

□ Use different shared secret for Accounting

□ Assume down if no keepalive packets after seconds

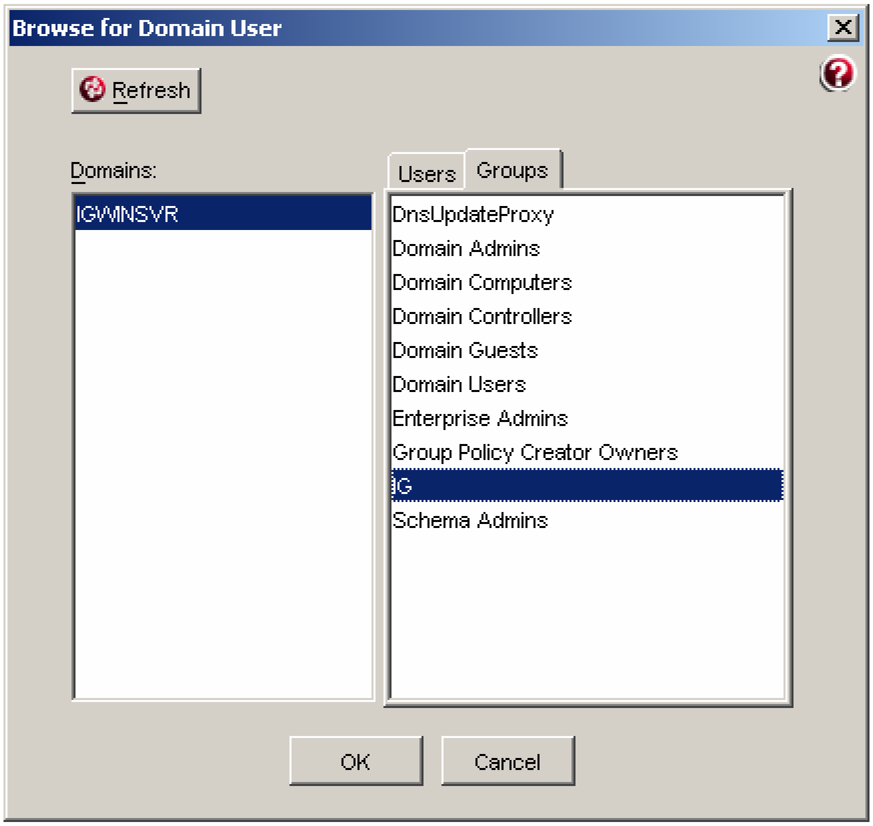
Next, click the **OK** button to save your changes and to return to the SBR Administrator Console.

4. Next, add a **Domain User.** Within the SBR Administrator Console, select the **Users** option within the left panel. Click the **Add** button within the toolbar above.



○ User ● Group

Select the **Group** option under the **Name** field and then click the **Browse** button. Select the Domain where your group user resides. In this example, the Domain is **IGWINSVR**. Next, select the **Groups** tab to list all security groups defined within the Domain. Select the group that will contain your users. In this example, the **IG** group is the group that contains the users targeted for Entrust IdentityGuard authentication.



Browse for Domain User

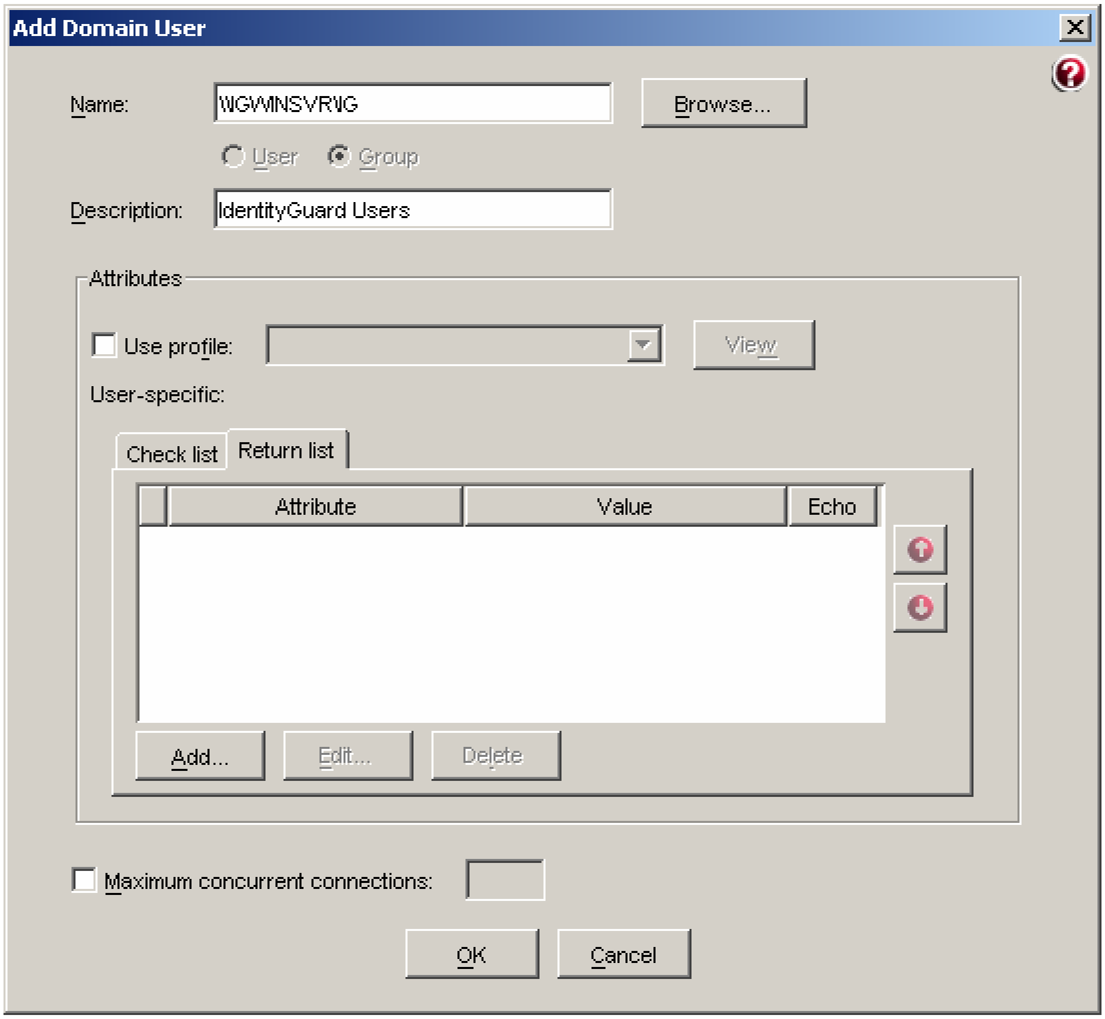
Domains:

IGWINSVR

DnsUpdateProxy
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Enterprise Admins
Group Policy Creator Owners
IG
Schema Admins

Click the **OK** button to save your selection and to exit the screen.

Click the **OK** button to save the Domain User and to exit back to the SBR Administrator Console.



Name: \IGWINSVR\IG

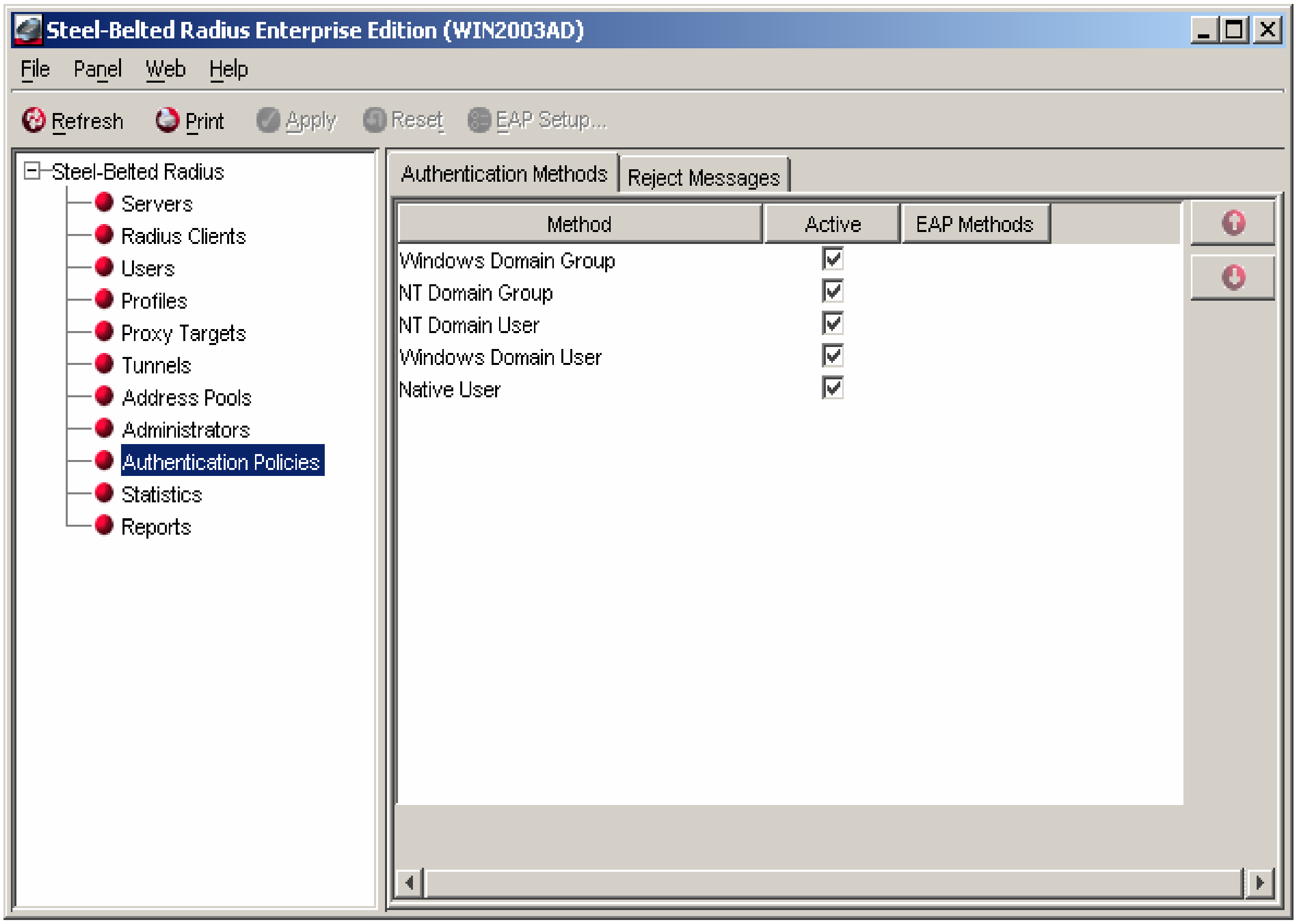
○ User ● Group

Description: IdentityGuard Users

□ Use profile:

□ Maximum concurrent connections:

5. To configure the authentication method, in the SBR Administrator’s console, select the Authentication Policies in the left pane. **Configuration** option button. Ensure that the authentication methods are selected in the correct order.



Method	Active	EAP Methods
Windows Domain Group	☑	
NT Domain Group	☑	
NT Domain User	☑	
Windows Domain User	☑	
Native User	☑	

Make sure that the **Windows Domain Group** has precedence over all other Methods by using the arrow buttons off to the far right to adjust up.

The Steel Belted Radius server is now configured to authenticate Check Point NG users using RADIUS authentication. Check Point NG will now be configured.

Configuration of Check Point Next Generation (R55 and R60)

IPSEC tunnels require that a secure session be established before any data exchange between client and switch. To establish such a session, a pre-shared key is required. The client will be authenticated against the external server (Funk Steel-belted Radius Server). The client's user name and password cannot be used to set up the tunnel since Check Point NG does not know the user ID or password (they are stored on the Active Directory, to which the external RADIUS server points).

To overcome this problem, the Group ID and Password (configured on both Check Point NG and the client) are used to create a secure session so that the user name and password can then be securely passed to the authentication server. In this way Check Point NG establishes the "outer" tunnel with the client using the Group ID to bind the tunnel to a particular group and the password as a pre-shared key. Once the "outer" tunnel is established, the clients' ID and password are verified against the external RADIUS server. (The actual user store is the Active Directory, to which the external RADIUS server points.) If RADIUS accepts the authentication, the user tunnel is established and the user can send/receive traffic, if RADIUS rejects the authentication, Check Point NG brings the tunnel down.

There are several Check Point NG Network Objects that must be configured to integrate IdentityGuard into the authentication process for end users. These are summarized below:

- Host Node
- RADIUS Server Object
- User Groups
- External User Profile

In addition, certain Global Properties of Check Point NG must be modified as well.

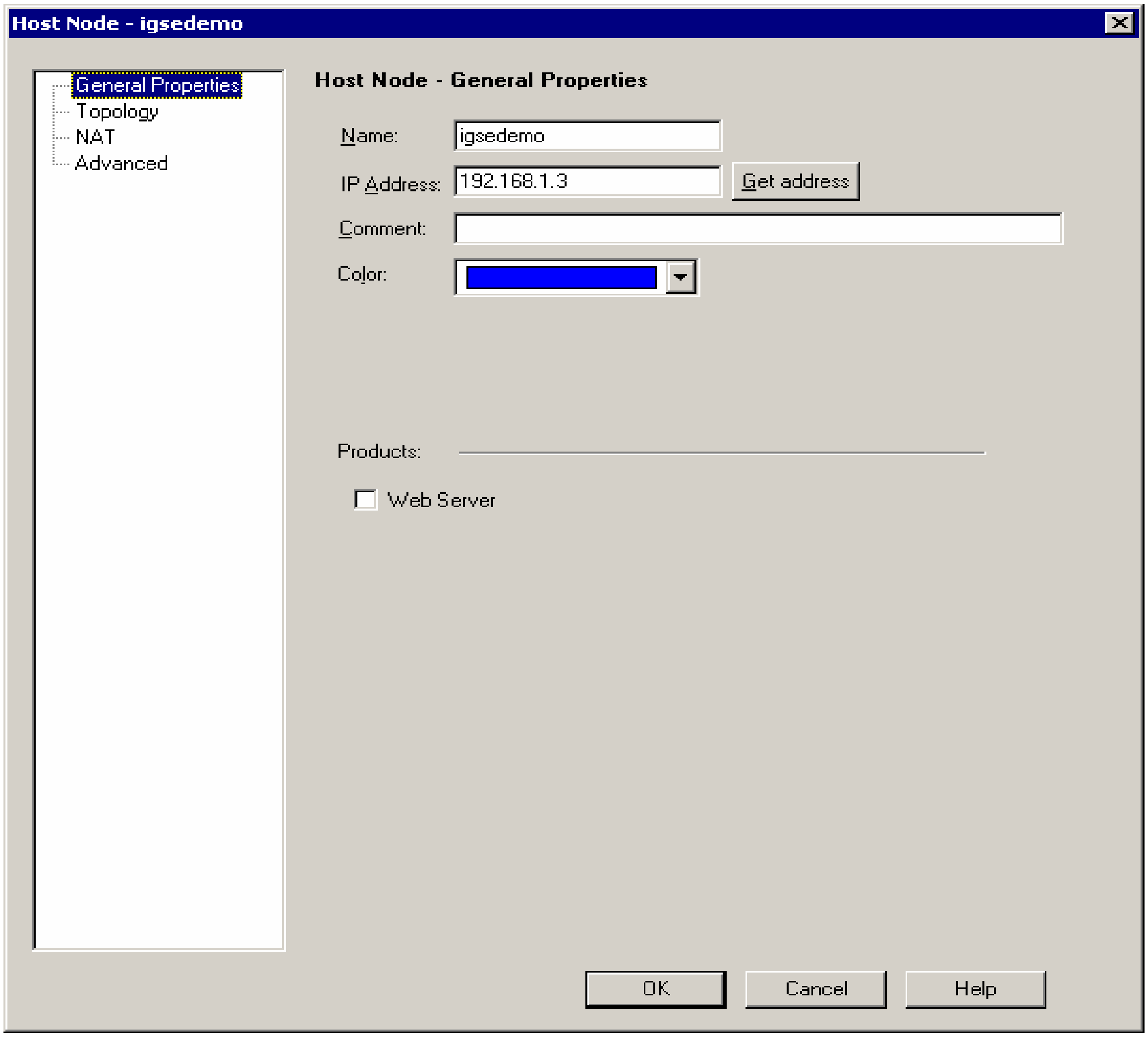
Once these changes have been made, Entrust IdentityGuard will provide two-factor authentication to those users tunnelling into Check Point NG.

Defining the Host Node

There are several steps that are necessary in defining a RADIUS server to Check Point NG. The first of which is to define the Host Node. Within the SmartDashboard Console, select the **Servers and OPSEC applications** object tree, select **Servers**, right click and select **New Host Node...**. Enter in the details of the new Host Node using the following as your guide:

- **Name** – A descriptive name for the Entrust IdentityGuard server. This must be unique.
- **IP Address** – The IP Address of the Entrust IdentityGuard server
- **Comment** – This is an optional field and allows you to add text to further describe your Entrust IdentityGuard server.
- **Color** – Allows for color coding Network Objects within the SmartDashboard. Follow internal standards or accept the default color.

Click the **OK** button to save your entry and exit the screen.



Name: igsedemo

IP Address: 192.168.1.3

Comment:

Color:

Products:

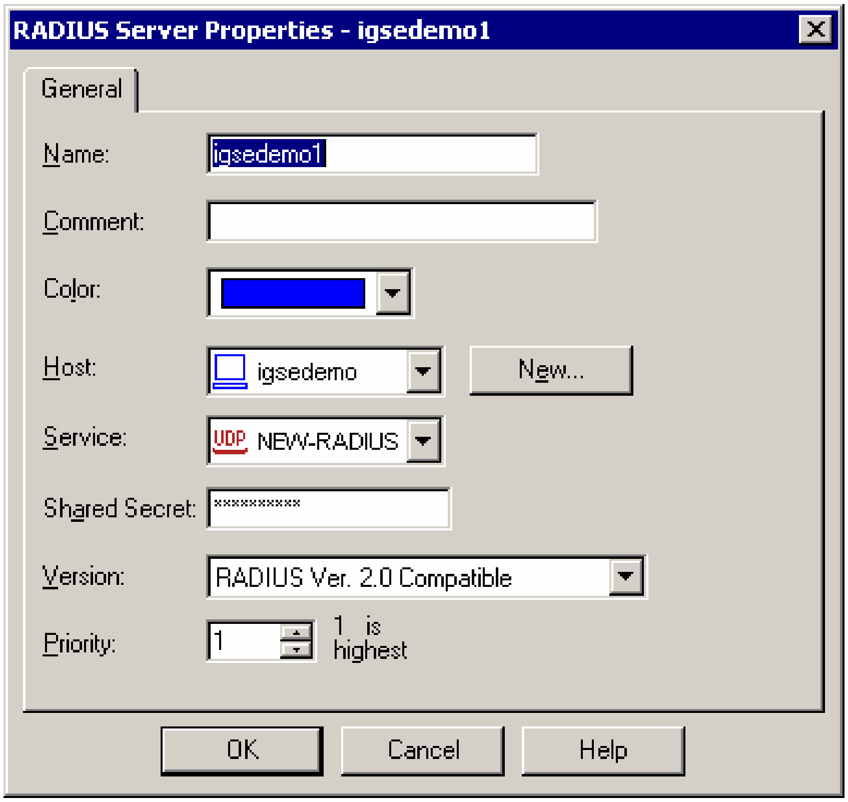
□ Web Server

Defining the RADIUS Server Object

Within the SmartDashboard console, define a new RADIUS Server object. In the **Servers and OPSEC applications** object tree, select **Servers**, right click and select **New RADIUS...**. Because Entrust IdentityGuard proxies all RADIUS communication to the real RADIUS server, we will enter the specifics of the Entrust IdentityGuard server when completing this step. Enter in the details that will describe the Entrust IdentityGuard server using the following as a guide:

- **Name** – A unique identifier given to the RADIUS Server object.
- **Comment** – An optional field further describing the RADIUS Server Object. Make sure you supply a comment to indicate that this is the Entrust IdentityGuard RADIUS proxy being defined.
- **Color** – Allows for color coding Network Objects within the SmartDashboard. Follow internal standards or take default color.
- **Host** – Describes the Host Node that will be associated with the RADIUS Server Object. Select the **Host Node** defined within the previous step. In this case, this will be **igsedemo**.
- **Service** – Select the appropriate RADIUS service. There are two possible selections: **RADIUS** and **NEW-RADIUS**. The RADIUS Service describes support for RADIUS running under port **1645** while NEW-RADIUS describes support for RADIUS running under port **1812**. If you selected the default RADIUS Port value during the Entrust IdentityGuard RADIUS proxy configuration then select **NEW-RADIUS** as your choice.
- **Shared Secret** – Enter the shared secret that will be used to allow for secure communication with the RADIUS Server. In this case, this will match the Shared Secret entered when you defined the RADIUS Client within the Funk RADIUS Server.
- **Version** – Select the **RADIUS Ver. 2.0 Compatible** choice from the selection list.
- **Priority** – Select the default value of 1. The Priority value is used to indicate which server gets priority when multiple RADIUS servers are defined.

Click the **OK** button when you are done to both save your configuration and return to SmartDashboard.



RADIUS Server Properties - igsedemo1

General

Name: igsedemo1

Comment:

Color:

Host: igsedemo

Service: NEW-RADIUS

Shared Secret: ***********

Version: RADIUS Ver. 2.0 Compatible

Priority: 1 1 is highest

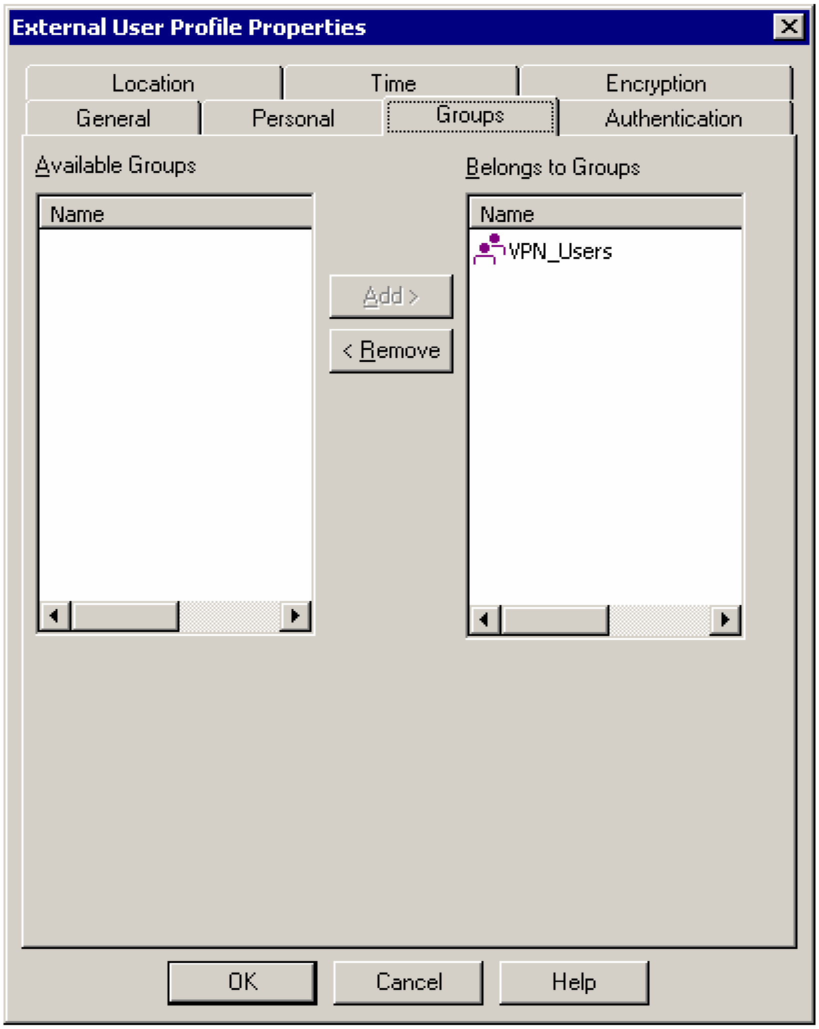
Defining the External User Profile

External User Profiles are profiles of externally defined users, that is, users who are not defined in the internal user's database or on an LDAP server. External user profiles are used to avoid the burden of maintaining multiple Users Databases, by defining a single, generic profile for all external users. External users are authenticated based on either their name or their domain.

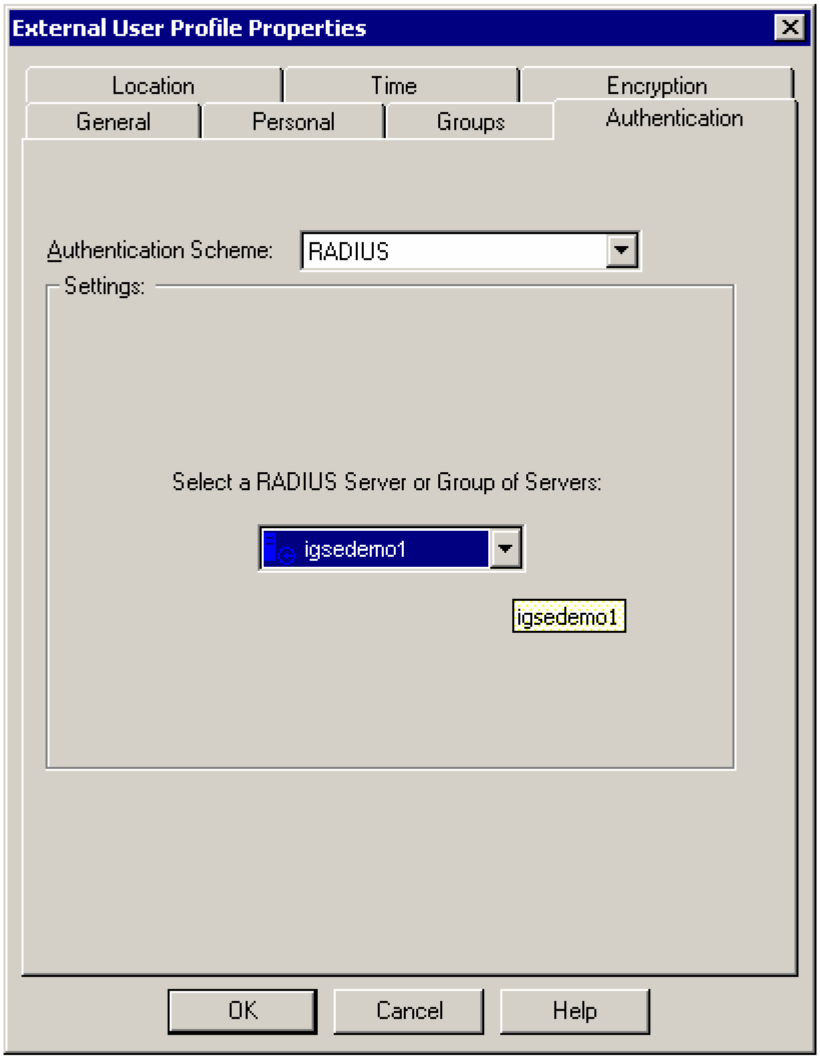
A User Group must be defined that will represent those users authenticating with Entrust IdentityGuard. Within the SmartDashboard console, define a new RADIUS Server object. In the **Users and Administrators** object tree, select **External User Profiles**, right click and select **New External User Profile** and then **Match all users...**. Several screens will be navigated to properly define the new External User Profile.

Once the External User Profile Properties window is displayed do the following:

- Select the **Group** tab and move the User Group defined earlier from the **Available Groups** list to the **Belongs to Groups** list. In our example, the **VPN_Users** group is selected and moved to the Belongs to Groups list.


External User Profile Properties
Location
Time
Encryption
General
Personal
Groups
Authentication
Available Groups
Name
Add >
< Remove
Belongs to Groups
Name
VPN_Users
OK
Cancel
Help

- Next, select the **Authentication** tab and select **RADIUS** as the Authentication Scheme. Within the Settings section, choose the RADIUS server that you defined earlier. In our example, this is **igsedemo1**.



Authentication Scheme: RADIUS

Settings:

Select a RADIUS Server or Group of Servers: igsedemo1

igsedemo1

This is all that is needed by Entrust IdentityGuard for the External User Profile. Proceed to the next section to complete the configuration of Check Point NG with Entrust IdentityGuard.

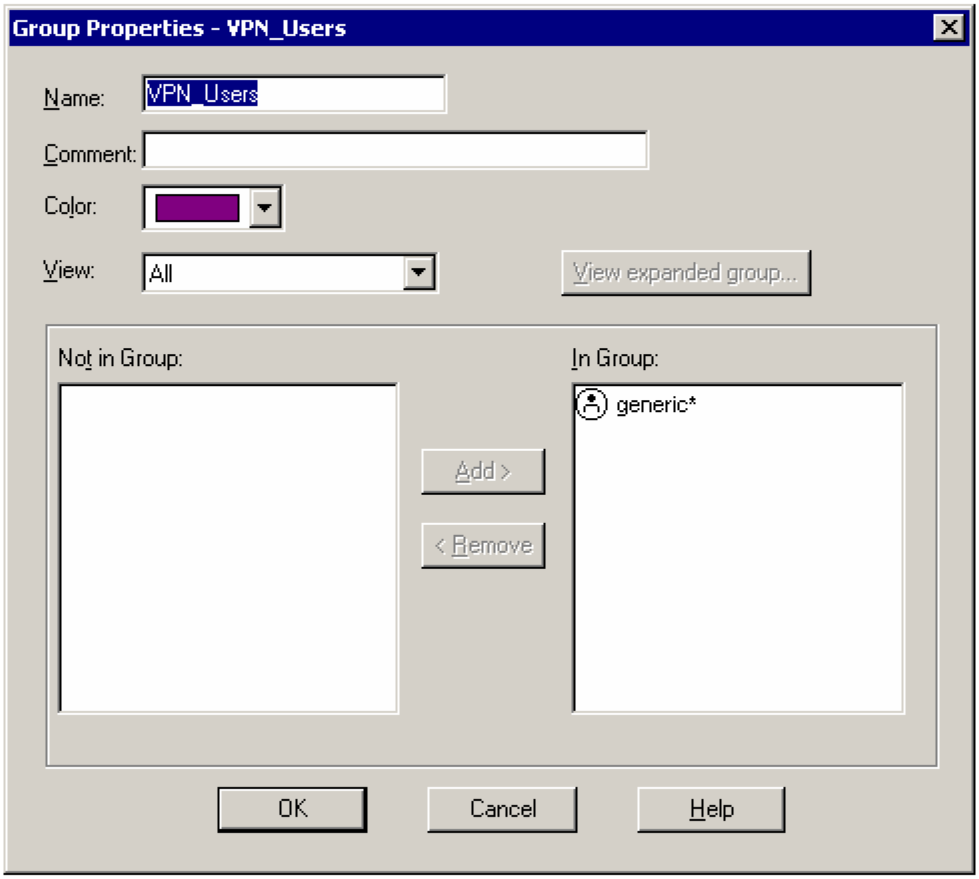
Defining the User Group

A User Group must be defined that will represent those users authenticating with Entrust IdentityGuard. Within the SmartDashboard console, define a new RADIUS Server object. In the **Users and Administrators** object tree, select **User Groups**, right click and select **New User Groups....** Enter in the details that will describe the Entrust IdentityGuard Server using the following as a guide:

- Name – Enter in a unique group name. Note that this is a required field and is case sensitive. In our example, we named this **VPN_Users**.
- Comment – Add additional text to describe the User Group
- Color – Allows for color coding Network Objects within the SmartDashboard. Follow internal standards or take default color.

Next, move the users, external user profiles or groups to be included in this group from the **Not in Group** list to the **In Group** list. In our case, we defined an External User Profile. In our example, we moved the External User Profile **generic*** to the **In Group** list.

Click **OK** to complete the definition.



Group Properties - VPN_Users

Name: VPN_Users

Comment:

Color: 🟪

View: All

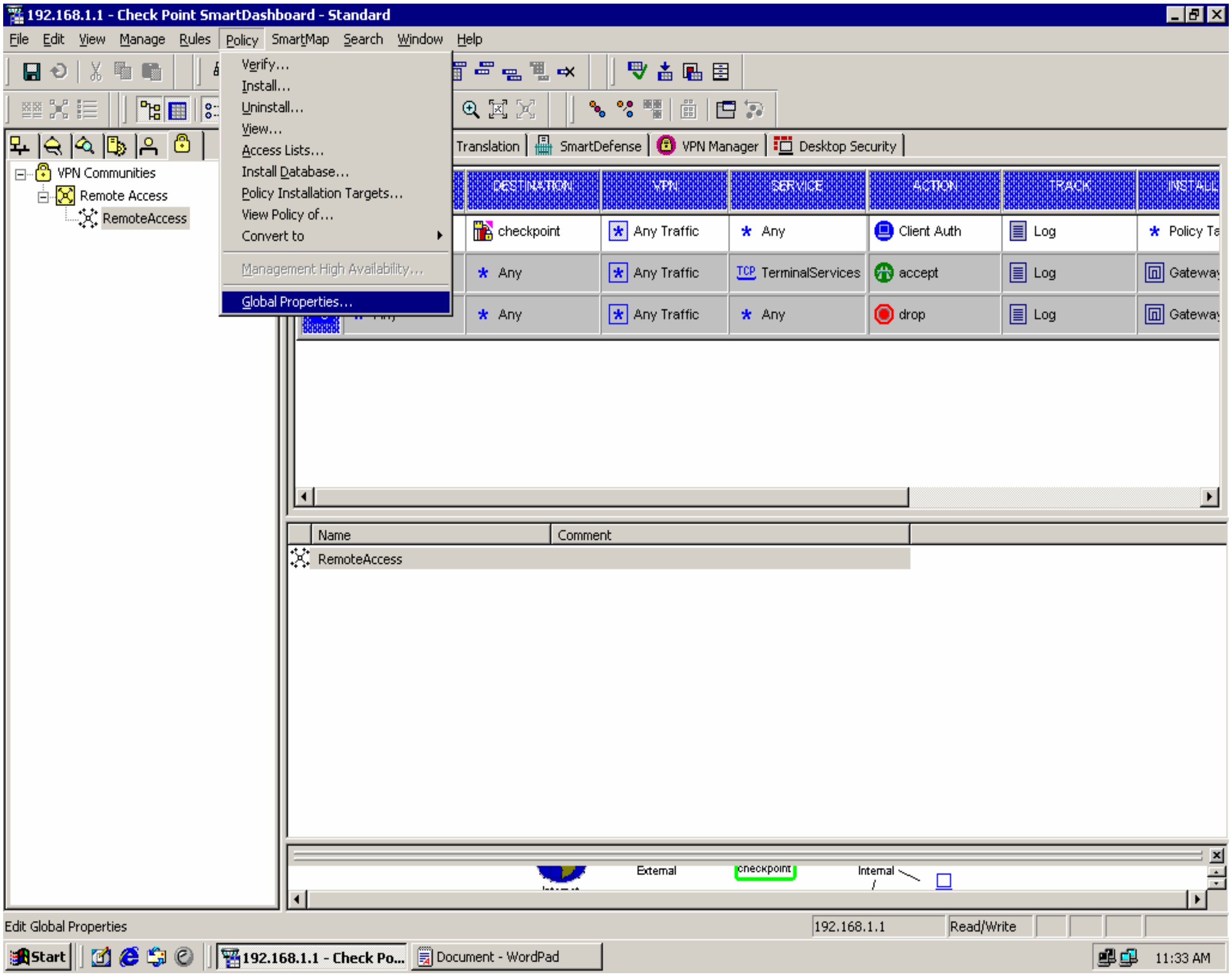
Not in Group:

In Group: generic*

Configuring the Global Properties

There are certain attributes within the Check Point NG Global Properties that must be checked to ensure a successful Entrust IdentityGuard integration. In order to support RADIUS authentication, Check Point NG must operate in Hybrid Mode and must be configured to ignore certain RADIUS attributes that Entrust IdentityGuard sends back. These configuration changes will be performed within this section.

Access the Global Properties section by selecting Policy from the toolbar and then choosing Global Properties option at the bottom.

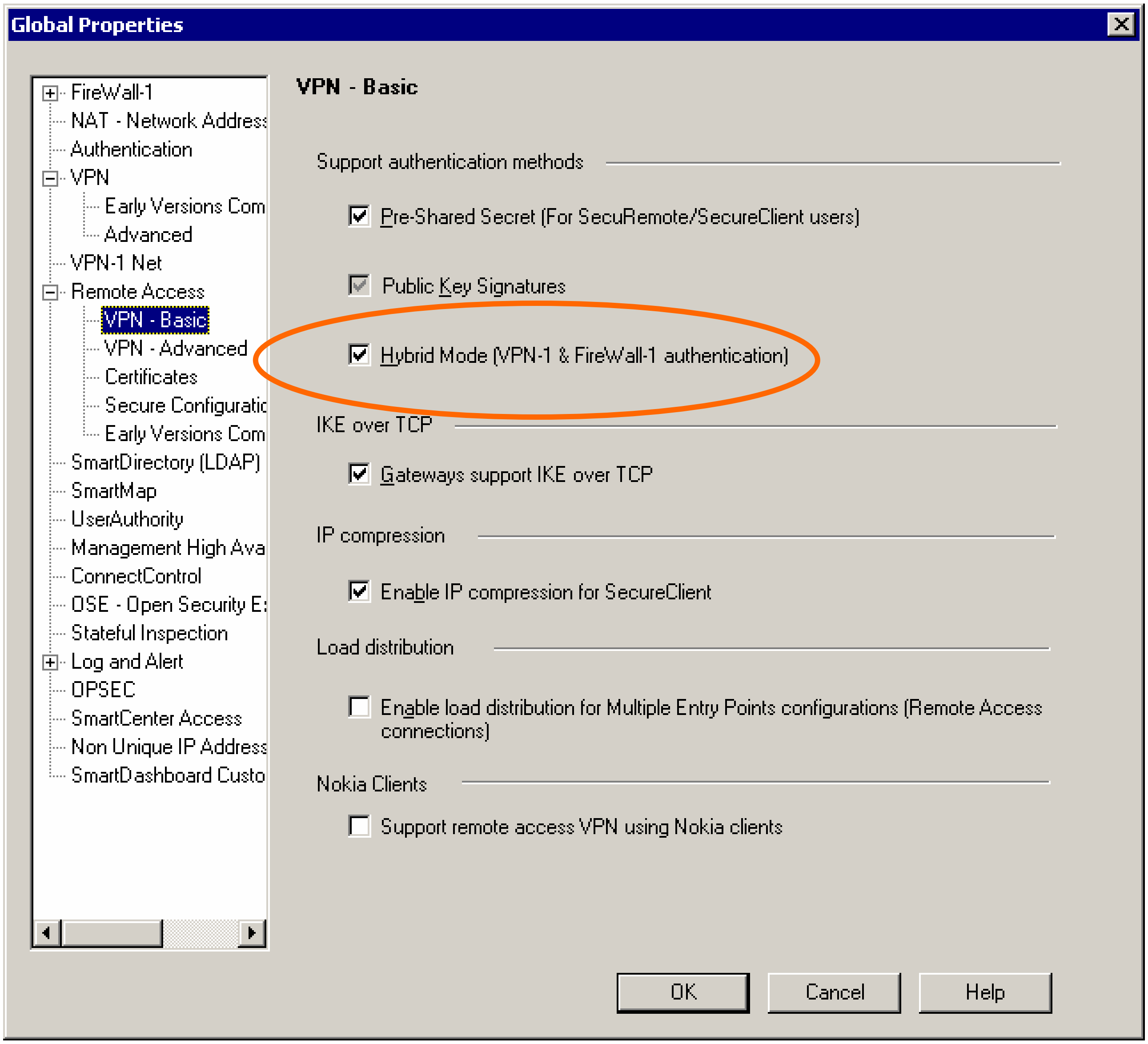


DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL
checkpoint	Any Traffic	Any	Client Auth	Log	Policy Ta
Any	Any Traffic	TCP TerminalServices	accept	Log	Gateway
Any	Any Traffic	Any	drop	Log	Gateway

Name	Comment
RemoteAccess	

Next, validate or configure the following:

- **Hybrid Mode** – Expand the **Remote Access** option and then select **VPN – Basic**. Make sure the **Hybrid Mode (VPN-1 & FireWall-1 authentication** option is selected. If not, for R55 select this option.



Global Properties

VPN - Basic

Support authentication methods

☑ Pre-Shared Secret (For SecuRemote/SecureClient users)

☑ Public Key Signatures

☑ Hybrid Mode (VPN-1 & FireWall-1 authentication)

IKE over TCP

☑ Gateways support IKE over TCP

IP compression

☑ Enable IP compression for SecureClient

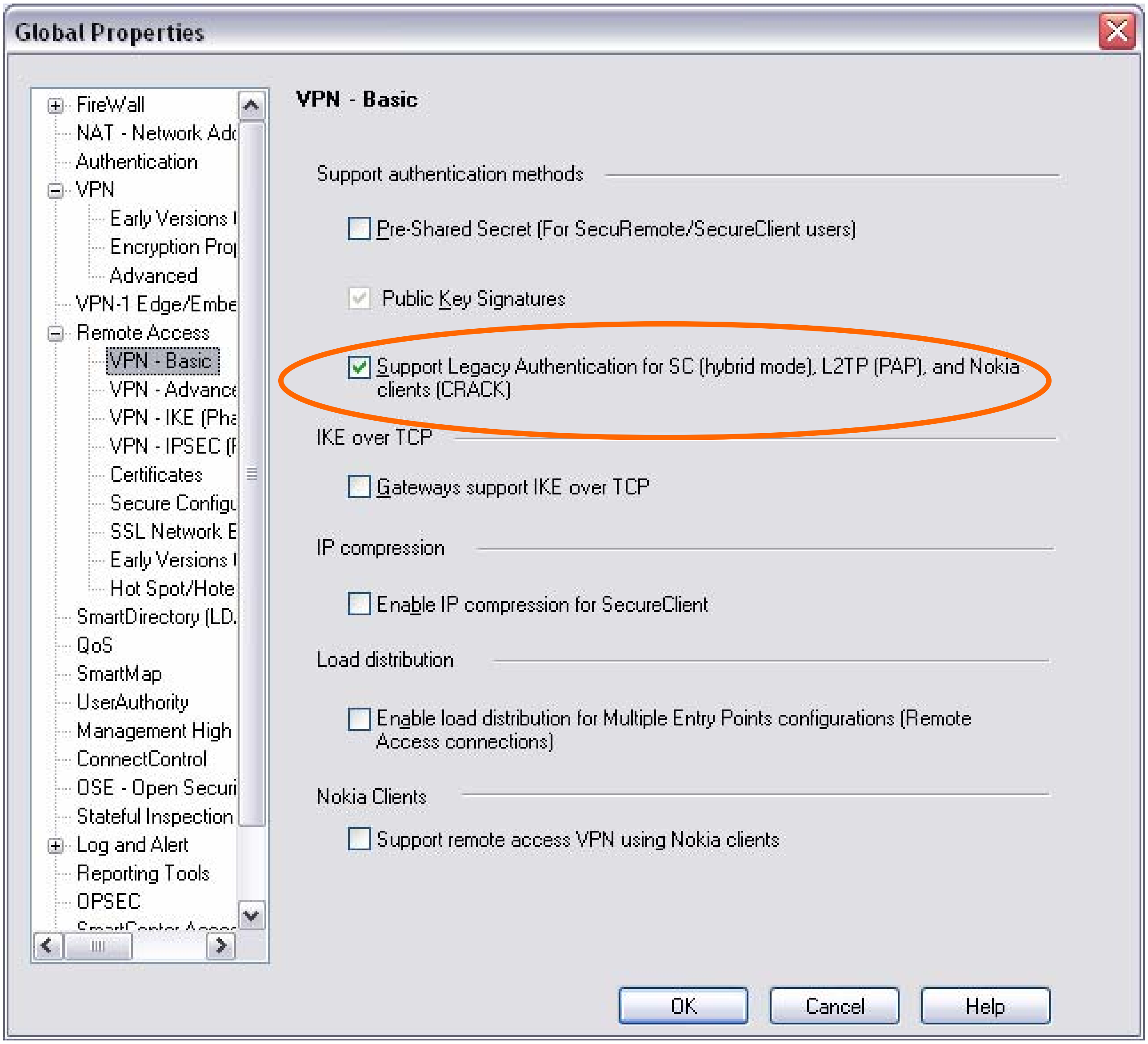
Load distribution

☐ Enable load distribution for Multiple Entry Points configurations (Remote Access connections)

Nokia Clients

☐ Support remote access VPN using Nokia clients

For R60 the display has been modified slightly and you will need to select this option



VPN - Basic

Support authentication methods

□ Pre-Shared Secret (For SecuRemote/SecureClient users)

☑ Public Key Signatures

☑ Support Legacy Authentication for SC (hybrid mode), L2TP (PAP), and Nokia clients (CRACK)

IKE over TCP

□ Gateways support IKE over TCP

IP compression

□ Enable IP compression for SecureClient

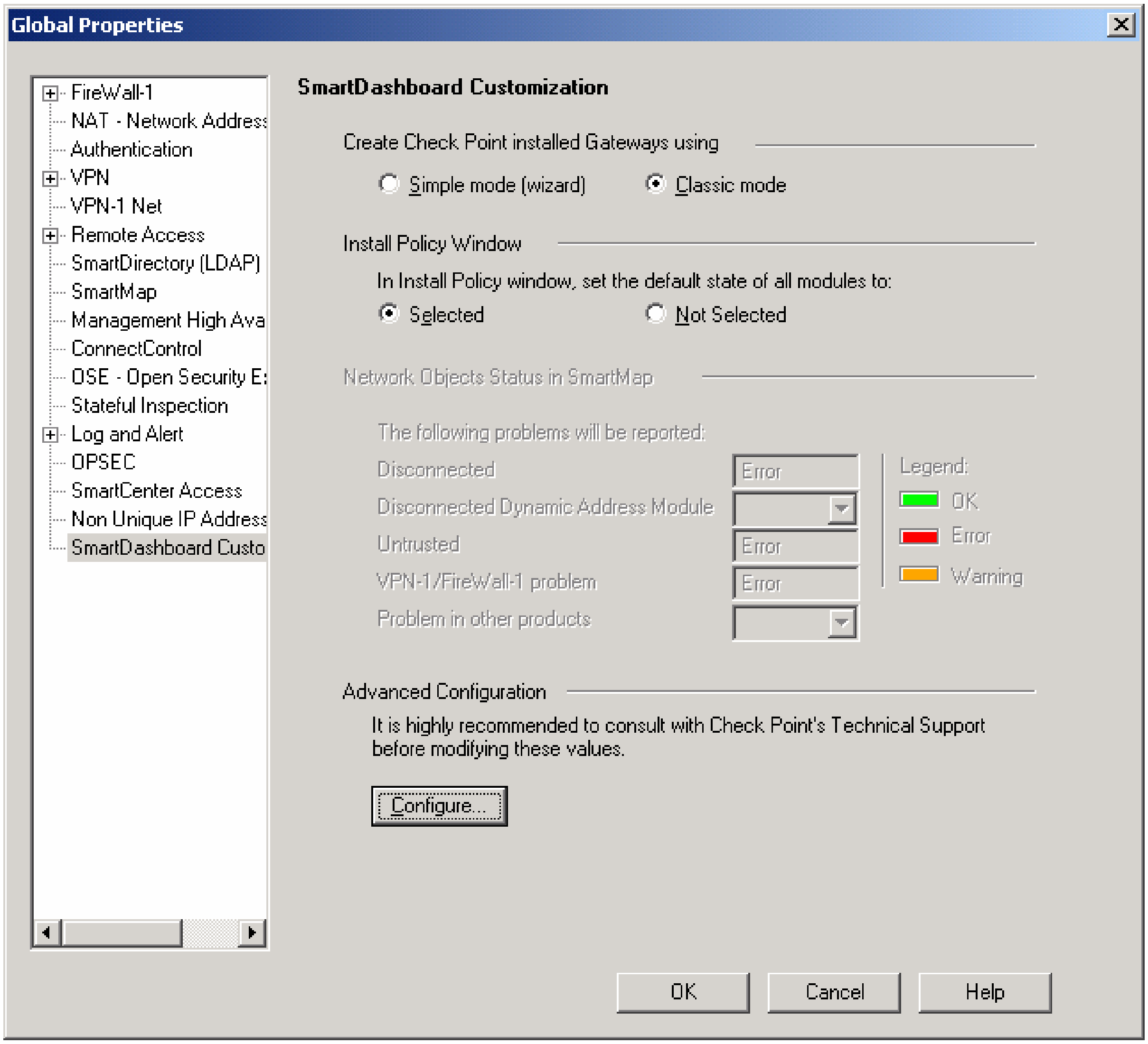
Load distribution

□ Enable load distribution for Multiple Entry Points configurations (Remote Access connections)

Nokia Clients

□ Support remote access VPN using Nokia clients

Ignore RADIUS Attribute 80 – Check Point NG only recognizes RADIUS attributes from 1 to 63 as defined within RFC 2138 (http://www.ietf.org/rfc/rfc2865.txt). Because Entrust IdentityGuard returns RADIUS attribute 80, Check Point NG must be told to ignore it otherwise this response will be blocked and the IdentityGuard authentication will fail. To have Check Point NG ignore RADIUS attribute 80, select **SmartDashboard Customization** at the bottom of the Global Properties window.



Global Properties

SmartDashboard Customization

Create Check Point installed Gateways using

○ Simple mode (wizard) ● Classic mode

Install Policy Window

In Install Policy window, set the default state of all modules to:

● Selected ○ Not Selected

Network Objects Status in SmartMap

The following problems will be reported:

Disconnected	Error
Disconnected Dynamic Address Module	
Untrusted	Error
VPN-1/FireWall-1 problem	Error
Problem in other products	

Legend:

🟩 OK
🟥 Error
🟧 Warning

Advanced Configuration

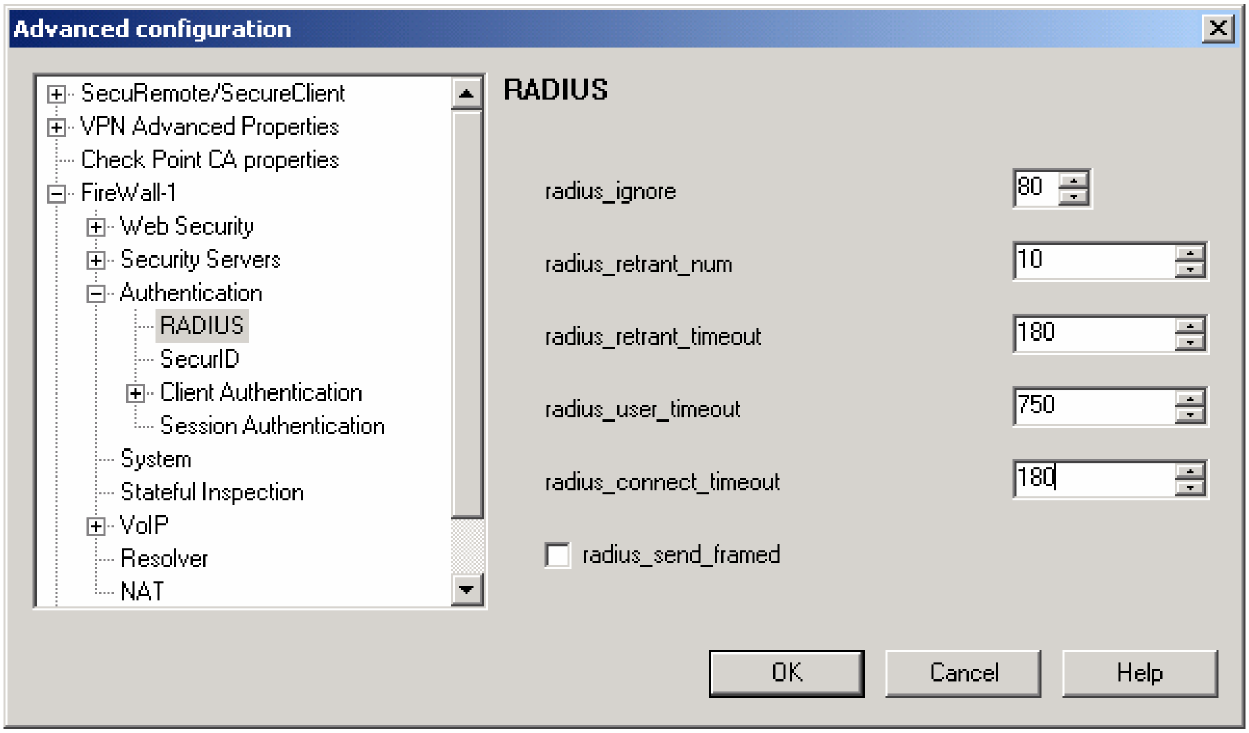
It is highly recommended to consult with Check Point's Technical Support before modifying these values.

Next, click the **Configure** button at the bottom of the window. Under **FireWall-1**, expand the **Authentication** section and then select **RADIUS** to expose all attributes. Update the radius_ignore attribute as follows:

- **radius_ignore** – Change this from **0** to **80.** This will instruct Check Point NG to ignore RADIUS Attribute 80 if it sees it. This allows the IdentityGuard challenge to be displayed to the end user by the Check Point SecurRemote Client.

Also, consider increasing the timeout values related to RADIUS authentication. These attributes were increased to take into account that Entrust IdentityGuard is now part of the RADIUS authentication process.

- **radius_retrant_num** – Change from **2** to **10.**
- **radius_retrant_timeout** – Change timeout value from **120** to **180.**
- **radius_user_timeout –** Change from **600** to **750**
- **radius_connect_timeout –** Change from **120** to **180**.



RADIUS

radius_ignore 80

radius_retrant_num 10

radius_retrant_timeout 180

radius_user_timeout 750

radius_connect_timeout 180

☐ radius_send_framed

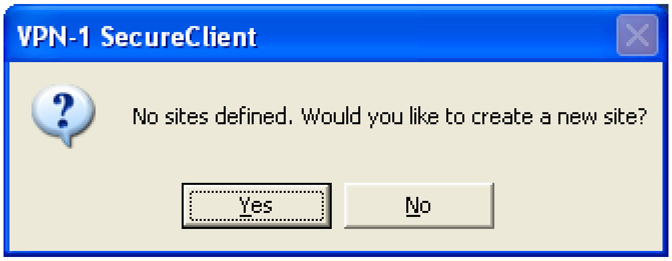
Note: For R60 in addition to the above configuration steps for ignoring the RADIUS attributes you must also obtain and apply a special patch. The patch is “HF_HA01_076” and can be applied on NGX HFA1. It will be available in HFA2 as well.

Configuring the Check Point SecureClient (R60)

Check Point offers two clients as part of its IPSEC VPN solution: SecureClient and SecuRemote. This document will describe the configuration of the Check Point SecureClient with Entrust IdentityGuard.

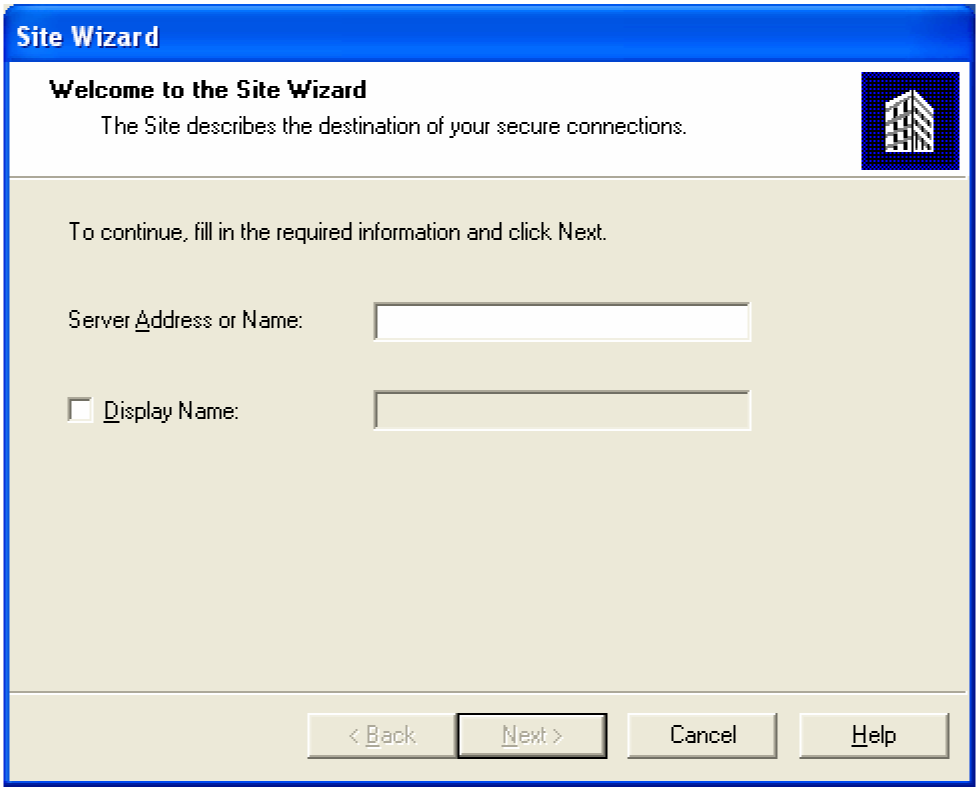
Note: The Site Wizard leverages user authentication to help in configuring a new Check Point Site. Make sure that the user name that you use in the Site Wizard exists within Active Directory and that this same user exists within Entrust IdentityGuard with the same user name. In addition to the user having a valid IdentityGuard user name, the user must have an active grid/card associated with their account. See the Entrust IdentityGuard Administration guide for more details on creating IdentityGuard users.

1. Start the **Check Point SecureClient,** select the **Sites** menu option and then **Create New.** If no **Sites** are defined, you will be asked if you want to create a new site. Click the **Yes** button.



No sites defined. Would you like to create a new site?

2. Enter the IP address of the Check Point NG server that this client will be connecting to.

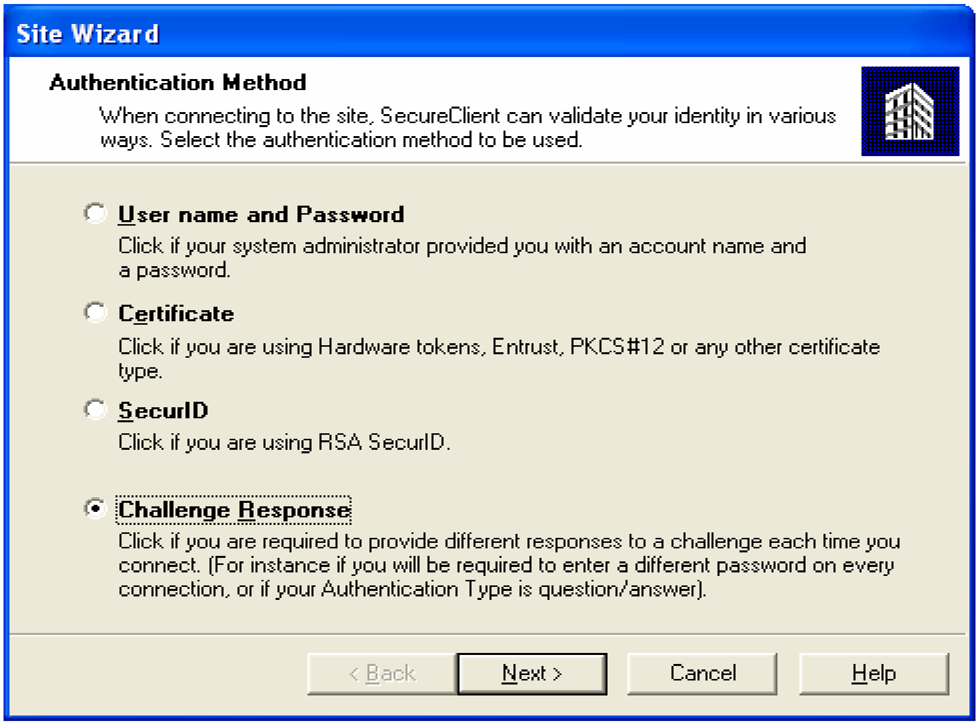


Welcome to the Site Wizard

The Site describes the destination of your secure connections.

To continue, fill in the required information and click Next.

3. Next, choose the Authentication Method to be used. To leverage Entrust IdentityGuard, choose the **Challenge Response** as your Authentication Method.



Site Wizard

Authentication Method

When connecting to the site, SecureClient can validate your identity in various ways. Select the authentication method to be used.

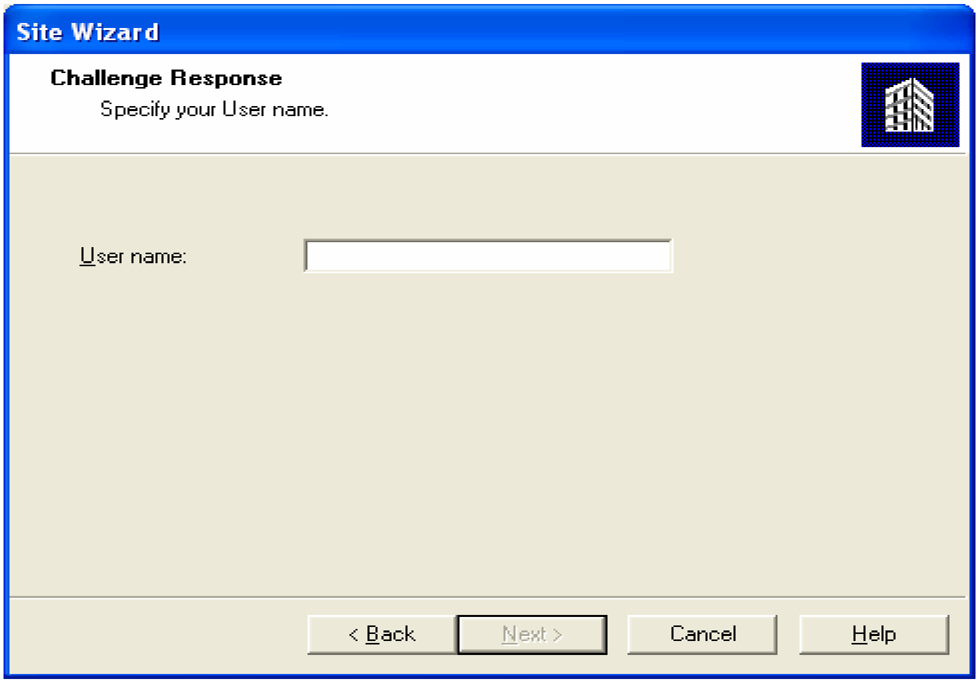
○ **User name and Password**
Click if your system administrator provided you with an account name and a password.

○ **Certificate**
Click if you are using Hardware tokens, Entrust, PKCS#12 or any other certificate type.

○ **SecurID**
Click if you are using RSA SecurID.

● **Challenge Response**
Click if you are required to provide different responses to a challenge each time you connect. (For instance if you will be required to enter a different password on every connection, or if your Authentication Type is question/answer).

4. Next, enter your User Name. Since the RADIUS server has been configured to authenticate users against Active Directory, this will essentially be your Active Directory or Windows user id.



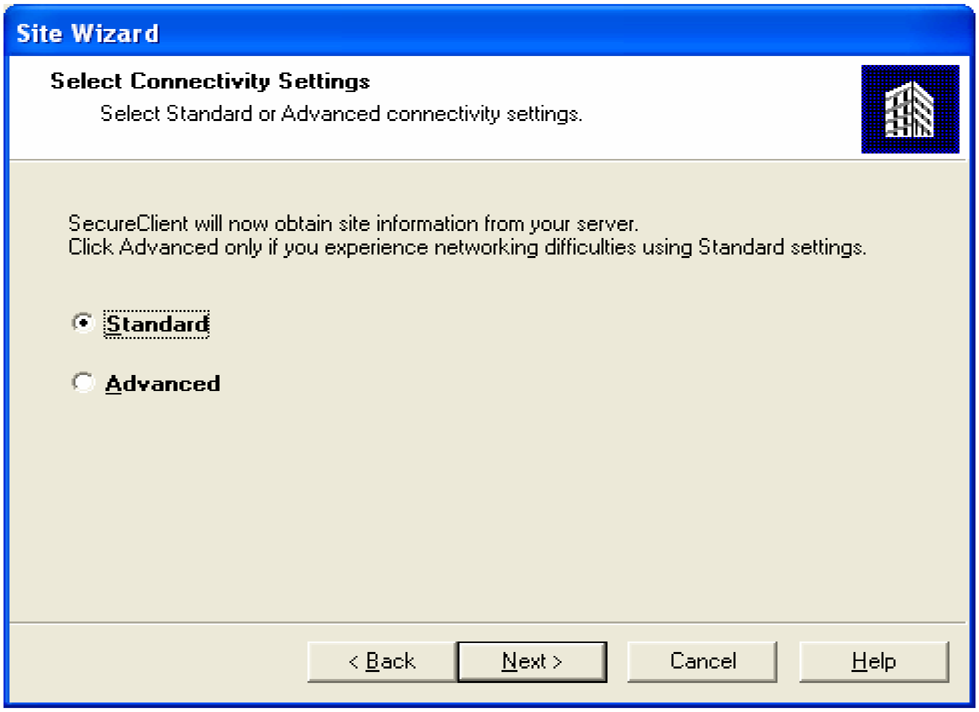
Site Wizard

Challenge Response

Specify your User name.

User name:

5. Next, choose your connectivity settings option. In most deployments, the **Standard** option will suffice.



Site Wizard

Select Connectivity Settings

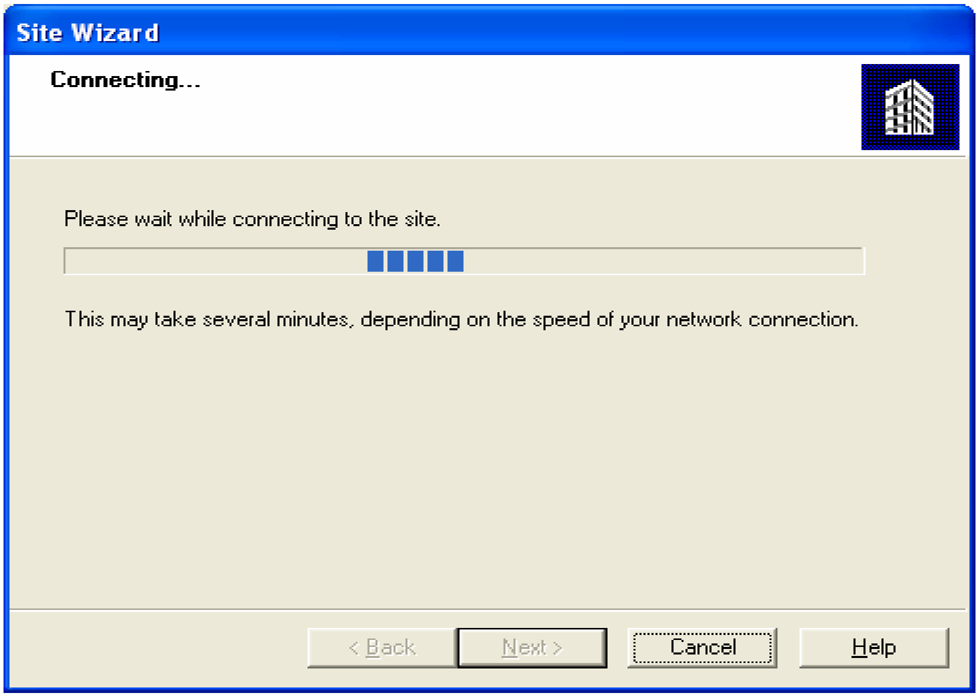
Select Standard or Advanced connectivity settings.

SecureClient will now obtain site information from your server.
Click Advanced only if you experience networking difficulties using Standard settings.

● Standard

○ Advanced

6. Check Point SecureClient has all the information needed to attempt a connection with the new site being configured.



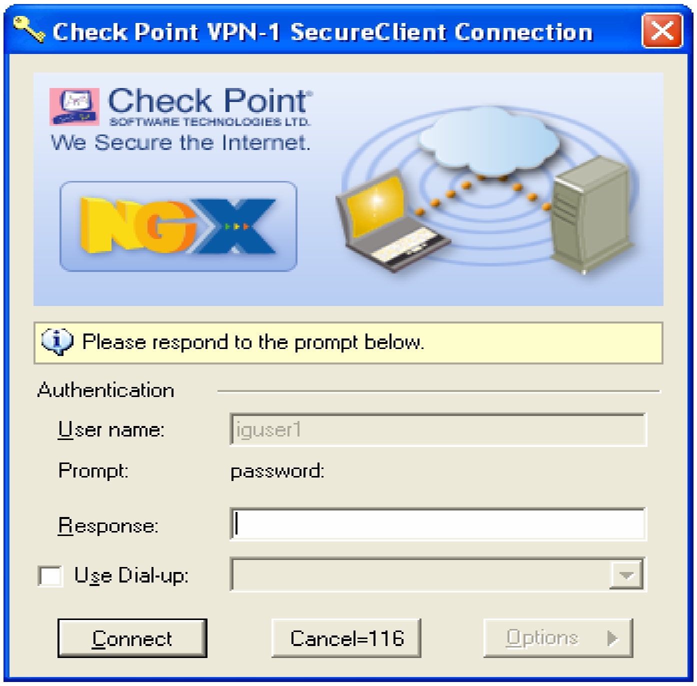
Site Wizard

Connecting...

Please wait while connecting to the site.

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

7. The Site Configuration Wizard requires that the user authenticate. Because Entrust IdentityGuard is now part of the authentication process, the user will be asked to authenticate not only against RADIUS, but also Entrust IdentityGuard.



Check Point VPN-1 SecureClient Connection

Please respond to the prompt below.

Authentication

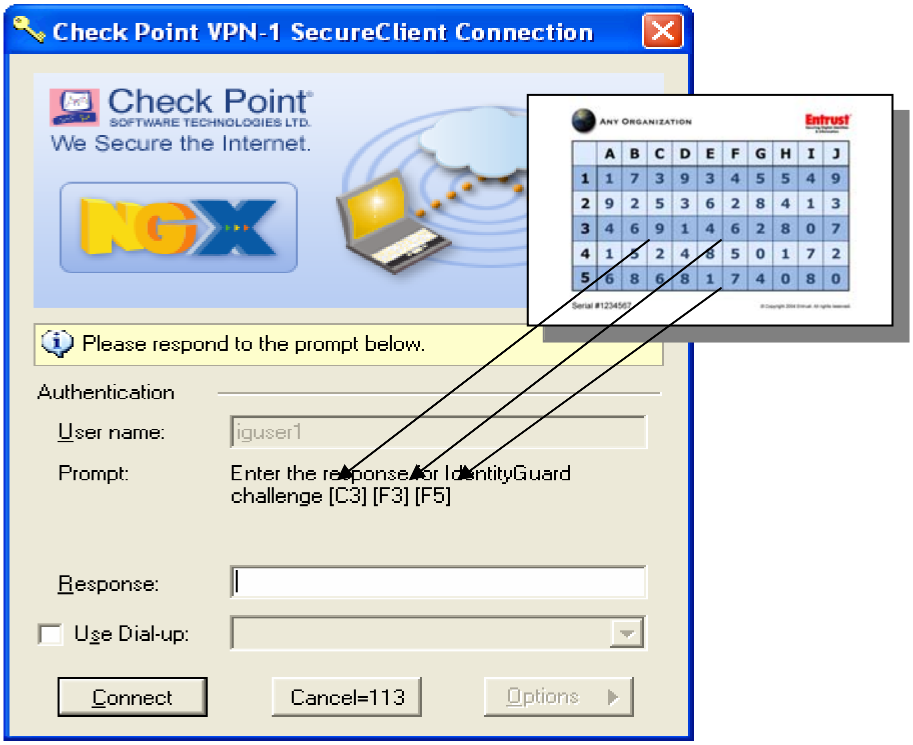
User name: iguser1

Prompt: password:

Response:

□ Use Dial-up:

The Entrust IdentityGuard challenge is presented to complete the 2nd factor of authentication.



Check Point VPN-1 SecureClient Connection

	A	B	C	D	E	F	G	H	I	J
1	1	7	3	9	3	4	5	5	4	9
2	9	2	5	3	6	2	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	1	5	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	0

Serial #1234567

Please respond to the prompt below.

Authentication

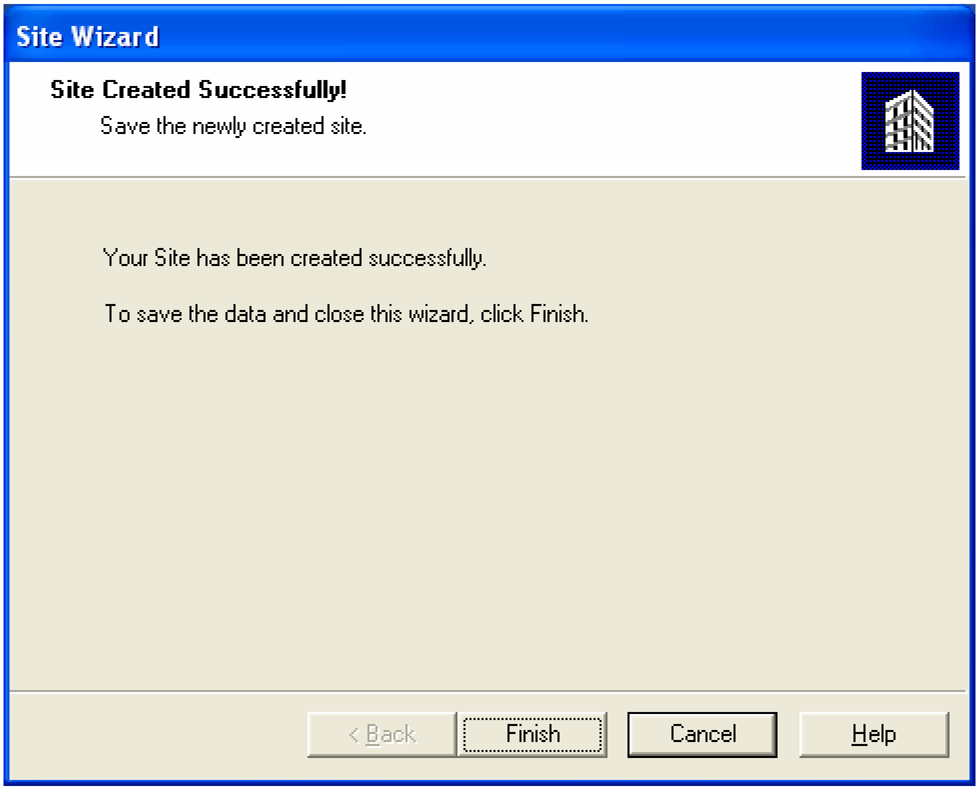
User name: iguser1

Prompt: Enter the response for IdentityGuard challenge [C3] [F3] [F5]

Response:

□ Use Dial-up:

8. Upon a successful authentication, the Site Wizard indicates that the site was created successfully. Click the **Finish** button to save the Site data and close the wizard.

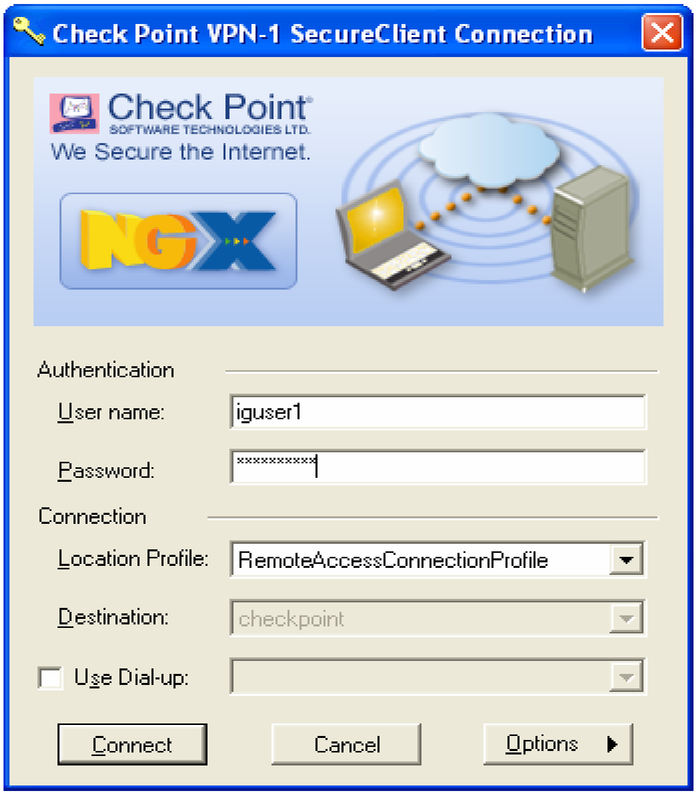


Your Site has been created successfully.

To save the data and close this wizard, click Finish.

Testing the Solution with Entrust IdentityGuard 7.2

1. Start the **Check Point VPN-1 SecureRemote Client**. Enter the user name and password for the user **iguser1** that you created in step 1. Click **Connect**.



Check Point VPN-1 SecureClient Connection
Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.
NGX
Authentication
Connection
Connect
Cancel
Options

User name: iguser1

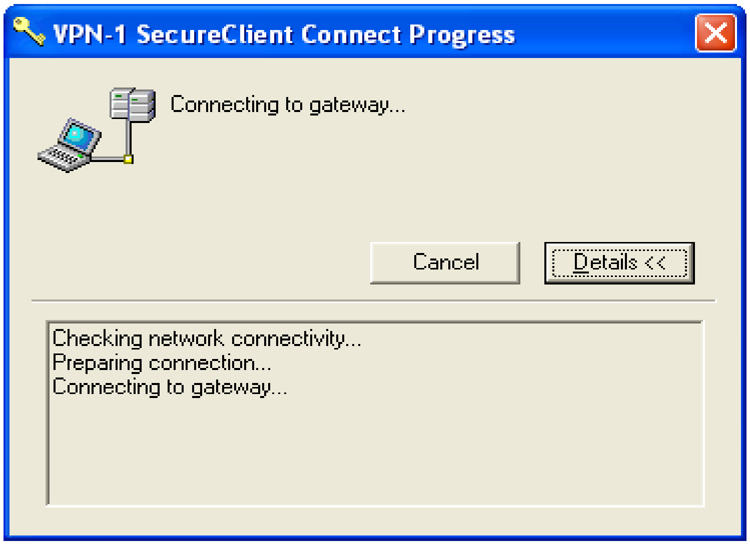
Password: ***********

Location Profile: RemoteAccessConnectionProfile

Destination: checkpoint

□ Use Dial-up:

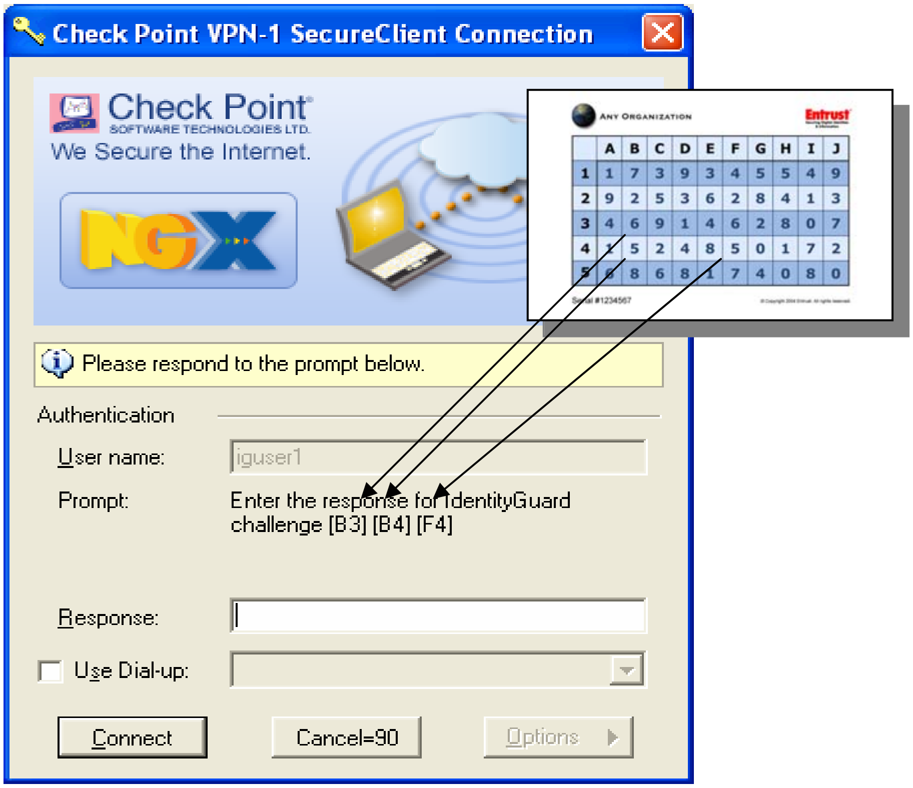
SecureClient displays the progress of the connection.



Connecting to gateway...

Checking network connectivity...
Preparing connection...
Connecting to gateway...

2. Next, the user is prompted for their grid coordinates found on their unique Entrust IdentityGuard grid or card. Enter the corresponding values to the grid coordinates displayed into the **Response** field. Click the **Connect** button to submit these to IdentityGuard for validation.



Check Point VPN-1 SecureClient Connection

Please respond to the prompt below.

Authentication

User name: iguser1

Prompt: Enter the response for IdentityGuard challenge [B3] [B4] [F4]

Response:

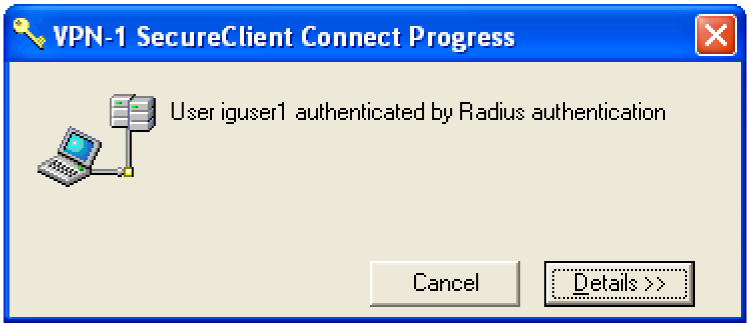
☐ Use Dial-up:

Any Organization

	A	B	C	D	E	F	G	H	I	J
1	1	7	3	9	3	4	5	5	4	9
2	9	2	5	3	6	2	8	4	1	3
3	4	6	9	1	4	6	2	8	0	7
4	1	5	2	4	8	5	0	1	7	2
5	6	8	6	8	1	7	4	0	8	0

Serial #1234567

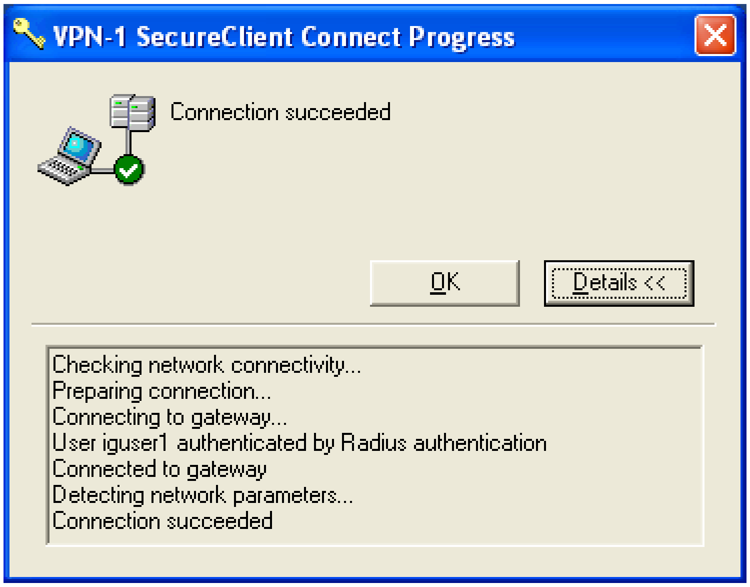
Check Point NG displays the progress of the Entrust IdentityGuard authentication.



VPN-1 SecureClient Connect Progress

User iguser1 authenticated by Radius authentication

3. The following dialog box is displayed indicating that the user authentication was successful using Entrust IdentityGuard. Click **OK** to continue.



Connection succeeded

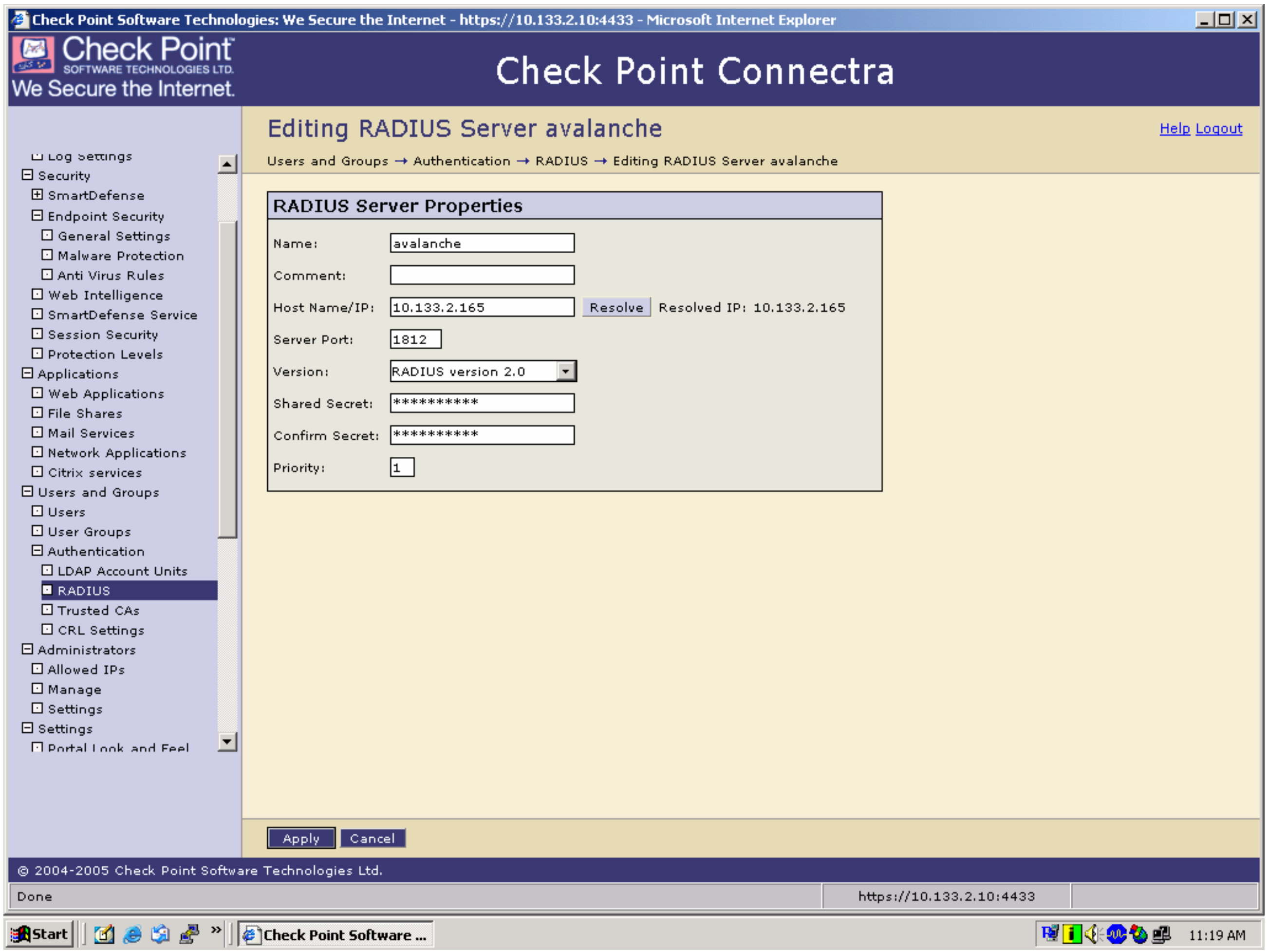
```
Checking network connectivity...
Preparing connection...
Connecting to gateway...
User iguser1 authenticated by Radius authentication
Connected to gateway
Detecting network parameters...
Connection succeeded
```

Note: SmartDashboard authentication does not work with IdentityGuard as it requires challenge.

Configuration and Testing of Check Point Connectra NGX

In order to make Entrust IdentityGuard work with Connectra the configuration is largely the same as outlined above. Specifically, the RADIUS server must be configured to communicate with the Entrust IdentityGuard server, the Connectra system must be configured to communicate via RADIUS with the Entrust IdentityGuard server and the RADIUS attribute 80 must be ignored.

In order to configure Connectra to communicate with the Entrust IdentityGuard server you will need to navigate within the Connectra administration portal to “Users and Groups -> Authentication -> RADIUS” and define a new object (in the below example the hostname avalanche at IP 10.133.2.165 is the Entrust IdentityGuard Server



Check Point Software Technologies: We Secure the Internet - https://10.133.2.10:4433 - Microsoft Internet Explorer

Check Point Connectra

Editing RADIUS Server avalanche

Users and Groups → Authentication → RADIUS → Editing RADIUS Server avalanche

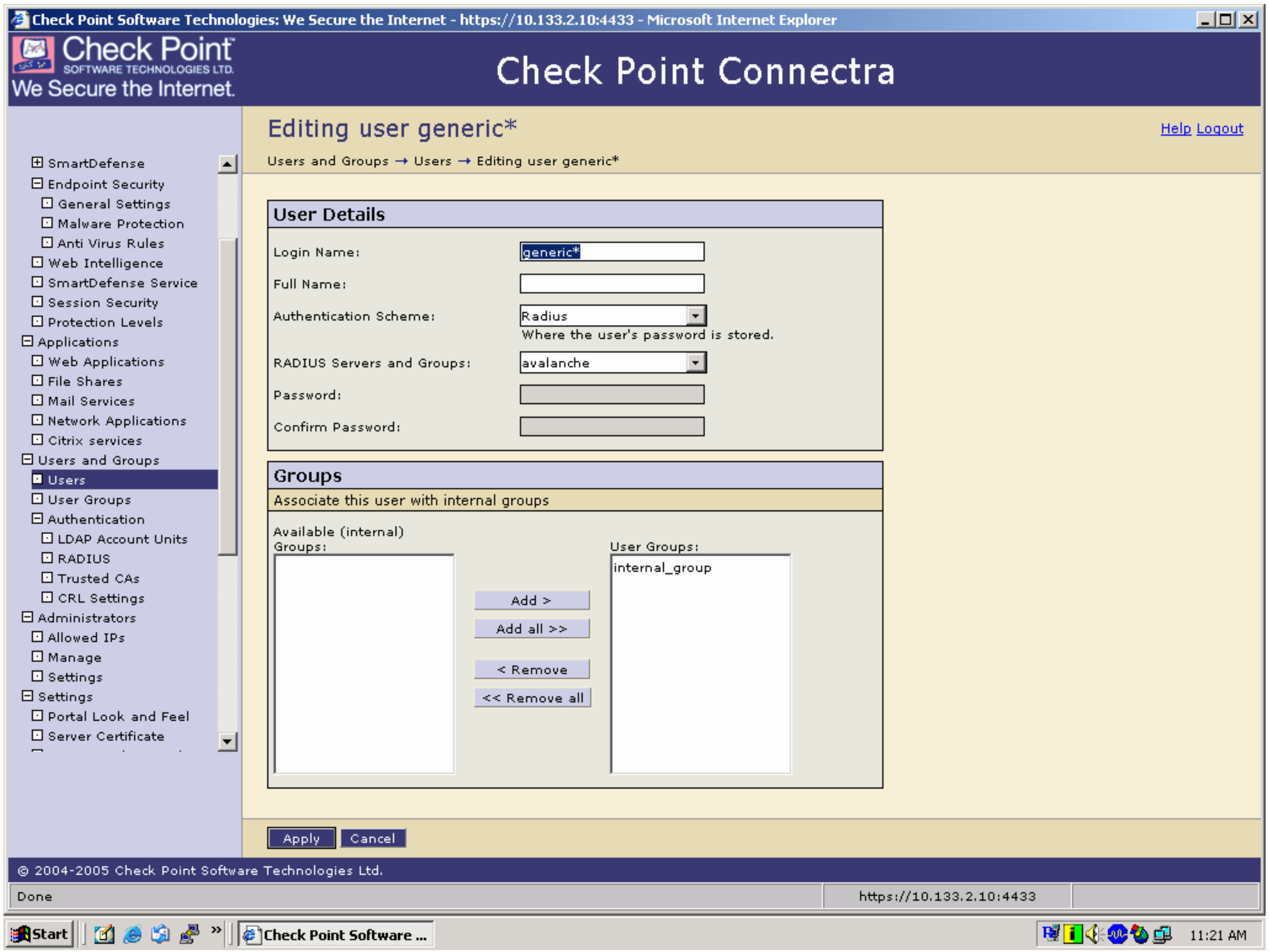
RADIUS Server Properties

Name:	avalanche
Comment:	
Host Name/IP:	10.133.2.165 Resolve Resolved IP: 10.133.2.165
Server Port:	1812
Version:	RADIUS version 2.0
Shared Secret:	**********
Confirm Secret:	**********
Priority:	1

© 2004-2005 Check Point Software Technologies Ltd.

Done https://10.133.2.10:4433

Next define a generic* user to use the newly configured RADIUS server entry (see below example)



Check Point Software Technologies: We Secure the Internet - https://10.133.2.10:4433 - Microsoft Internet Explorer

Check Point Connectra

Editing user generic*

Users and Groups → Users → Editing user generic*

User Details

Login Name: generic*

Full Name:

Authentication Scheme: Radius

Where the user's password is stored.

RADIUS Servers and Groups: avalanche

Password:

Confirm Password:

Groups

Associate this user with internal groups

Available (internal) Groups:

User Groups: internal_group

© 2004-2005 Check Point Software Technologies Ltd.

Once this has been setup you will need to force the Connectra system to ignore RADIUS attribute 80, In order to do this login to the Connectra command line (via console, ssh etc.), enter 'Expert' mode and perform the following steps:.

a. Issue 'cpstop'
b. Make a backup copy of $FWDIR/conf/objects_5_0.C (i.e. cp $FWDIR/conf/objects_5_0.C /objects_backup.C
b. Edit $FWDIR/conf/objects_5_0.C (using vi, etc.)
c. Search for the following

```
:radius_groups_attr (25)
:radius_retrant_num (2)
```

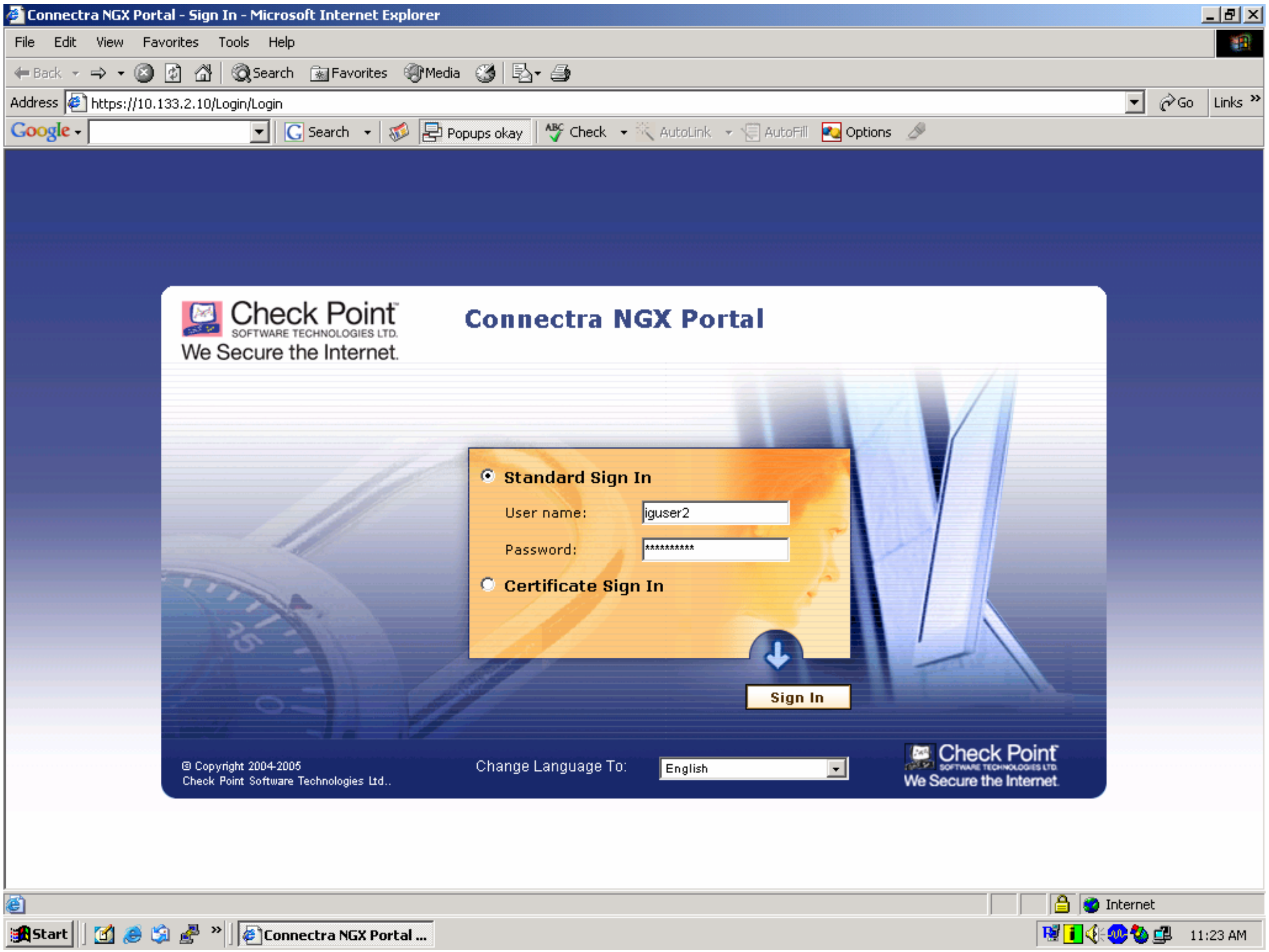
Change it to

```
:radius_groups_attr (25)
:radius_ignore (80)
:radius_retrant_num (2)
```

d. Save the file and issue 'cpstart'

Be very careful about syntax, extraneous characters etc. when editing objects_5_0.C – if you are at all uncertain about how to edit this file please contact Check Point Technical services for assistance.

Finally you can test the Connectra and Entrust IdentityGuard installation by logging into the user portal page (see below)


Connectra NGX Portal - Sign In - Microsoft Internet Explorer

Address https://10.133.2.10/Login/Login

Connectra NGX Portal

● Standard Sign In

User name: iguser2

Password: **********

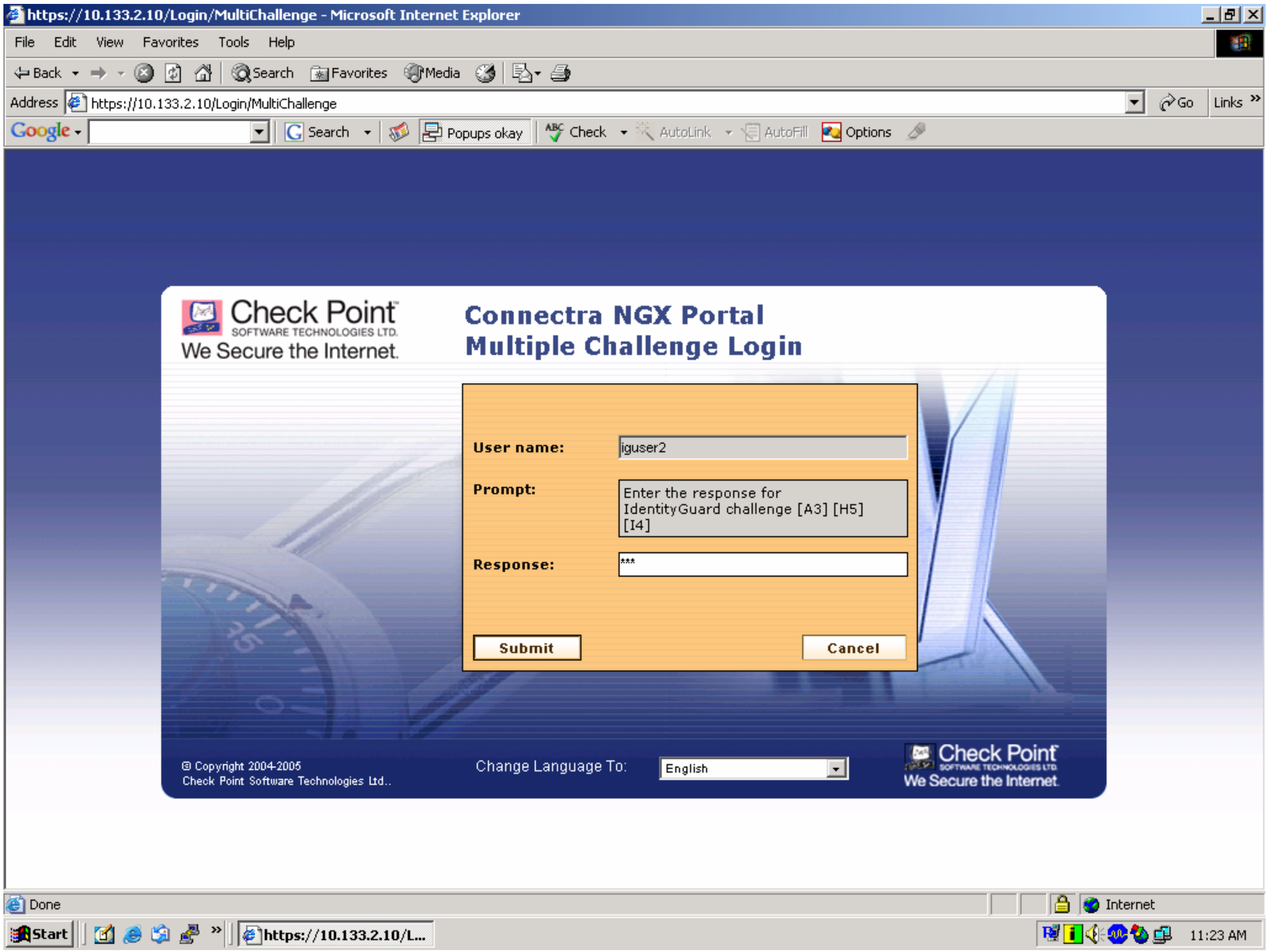
○ Certificate Sign In

Sign In

© Copyright 2004-2005
Check Point Software Technologies Ltd..

Change Language To: English

After providing the password you will be prompted for the Entrust IdentityGuard response which you can populate as discussed in the SecureClient R60 section above;



https://10.133.2.10/Login/MultiChallenge - Microsoft Internet Explorer

Connectra NGX Portal
Multiple Challenge Login

User name: iguser2

Prompt: Enter the response for IdentityGuard challenge [A3] [H5] [I4]

Response: ***

Change Language To: English

Note: Client authentication for 'non IPSEC/sslvpn' traffic (i.e. ftp, http,) can work in conjunction with IdentityGuard.

Entrust Product Information

Entrust IdentityGuard 7.2

Entrust IdentityGuard is a key component of the Entrust Secure Identity Management Solution. It provides a second factor of user authentication designed to help organizations counter identity theft by making it more difficult for attackers to steal user online identities.

With Entrust IdentityGuard, users continue to employ their current user name and password, but are also provided with a second physical form of authentication based on an assortment of characters in a row/column grid format printed on a card. A user must successfully complete a coordinate challenge to demonstrate that they are in possession of the appropriate card.

Partner Product Information

Partner Name: Check Point
Website: http://www.Check Point.com
Product Name: NG with Application Intelligence (R55)

Product Version: NG
Release Version: R55

Product description: Check Point NG with Application Intelligence (R55) is a tightly integrated firewall and VPN gateway that provides comprehensive security and remote connectivity for corporate applications and network resources. VPN-1 Pro combines the market-leading FireWall-1® security suite with sophisticated VPN technologies to meet the demanding requirements of Internet, intranet, and extranet VPNs by providing secure connectivity to corporate networks, remote and mobile users, branch offices, and business partners. It features the industry's most intelligent security inspection technologies, Stateful Inspection and Application Intelligence™, providing preemptive attack prevention against both network- and application layer attacks. VPN-1 Pro solutions are available on the industry's broadest range of open platforms and security appliances—meeting the price/performance requirements of any size organization.

Product Name: NGX
Release Version: R60

Delivering a unified security architecture for perimeter, internal and Web security, NGX is the latest security software platform for Check Point firewall, VPN and management solutions. This unique platform offers hundreds of new features and extended functionality. Check Point VPN-1 Pro provides you the most intelligent, reliable security for stopping attacks while simplifying business communications across the Internet. A tightly integrated combination of firewall, VPN and intrusion prevention, VPN-1 Pro is built on Stateful Inspection, Application Intelligence, and One-Click VPN technologies. SmartCenter, Check Point's centralized management solution, provides unified security management of your security infrastructure

http://www.checkpoint.com/products/vpn-1_pro/index.html

Product Name: Connectra
Product Version: NGX

Check Point Connectra™ is a complete Web Security Gateway that provides SSL VPN access and integrated endpoint and application security in a single, unified solution. By combining both connectivity and security in one solution, organizations can effectively deploy SSL VPNs safely and securely to a diverse set of users from the industry's most reliable provider of intelligent
security solutions.

http://www.checkpoint.com/products/downloads/connectra_datasheet.pdf

---

Partner Name: Funk Software Inc.
Website: http://www.funk.com
Product Name: Steel-belted Radius Server
Product Version: 4.71.739

Product description: The Funk Steel-Belted Radius is a complete implementation of the widely used RADIUS (Remote Authentication Dial-In User Service) protocol. It performs three vital functions:

- **Authentication** — validates any user's login credentials against a central security database to ensure that only individuals with valid credentials will be granted network access.
- **Authorization** — for each new connection, provides information to the network access device, such as what IP address to use, session time-limit information, or which type of tunnel to set up.
- **Accounting** — logs all connections, including user names and connection duration, for tracking and billing.

When a user connects to the network via a remote access server, VPN, firewall, router, access point, or any other RADIUS-compliant network access device, that device queries Steel-Belted Radius to determine if the user is authorized to connect. Steel-Belted Radius accepts or rejects the connection based on user credential information in the central security database, and authorizes the appropriate type of connection or service. When the user logs off, the network access device informs Steel-Belted Radius, which in turn records an accounting transaction.

System Components

Entrust IdentityGuard 7.2	• Check Point NG with Application Intelligence (R55), R60 or • Connectra NGX • Funk Steel-belted Radius Server

Partner Contact Information

Check Point Sales and Support Contact: http://www.Check Point.com/corporate/contact_list.html

Funk Sales and Support Contact: Trevor Failor, Manager, North America Channels, trevor@funk.com, (800) 828-4146, ext. 289

Please check PSIC for the latest supported version information at:
https://www.entrust.com/support/psic/index.cfm