

Entrust[®] Securing Digital Identities & Information



**Securing Your
Digital Life**

Technical Integration Guide for Entrust IdentityGuard 8.0 and
Nortel™ VPN Router CES1700D (Contivity)

Document issue: 1.0

December 2005

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. 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.

Copyright © 2005. Entrust. All rights reserved.

Contents

Introduction	1
Integration information	1
Prerequisites	1
Before you start.....	1
Installing and configuring Entrust IdentityGuard	2
RADIUS Integration overview	2
Integration details	3
Configuring the RADIUS server	3
Configuring the Nortel VPN Router (Contivity)	9
Configuration for Entrust IdentityGuard 8.0	14
Testing the configuration with Entrust IdentityGuard 8.0.....	17

Introduction

This technical integration guide documents how to integrate Nortel VPN Router CES1700D (Contivity) and Entrust IdentityGuard 8.0. The aim of this integration is to provide strong, second-factor authentication to your Nortel VPN solutions using Entrust IdentityGuard.

Entrust IdentityGuard can help increase the security of online identities and significantly improve an organization's resistance to identity theft attacks such as phishing. It addresses the real-world demands of strong authentication, making it easier to use while helping to reduce deployment and management costs.

The integration of Entrust IdentityGuard and a Nortel VPN solution requires a RADIUS server that supports challenge-response, an integral part of the RADIUS standard. To illustrate this integration, this document uses the Funk Steel-belted RADIUS server. You can use any RADIUS server that supports the RADIUS challenge response message.

This integration works with both Entrust IdentityGuard grid values and temporary PINs. For more information on using Entrust IdentityGuard 8.0, refer to the *Entrust IdentityGuard Administration Guide*.

Integration information

Partner name: Nortel Networks

Product name: Nortel VPN Router CES1700D (Contivity)

Product version: V05_05.117

Partner name: Funk Software Inc.

Product name: Steel-belted RADIUS Server

Product version: 4.71.739

Check the Platform Support and Integration Center for the latest supported version information at:

<https://www.entrust.com/support/psic/index.cfm>

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

Before configuring your authentication system to work with Entrust IdentityGuard, do the following:

- Make sure the target computer has either Windows 2000 Server or Windows 2003 Server with Domain Controller and Active Directory installed on it.
- Create a security group within Active Directory where you will create end users in a group called IG.
- If you decide to install the Steel-belted RADIUS Server on a regular domain computer, create a user account for that server within Active Directory.
- Install the Steel-belted RADIUS server, using the instructions provided by Funk Software.

Configuration includes:

- [“Installing and configuring Entrust IdentityGuard”](#)
- [“Configuring the RADIUS server”](#)
- [“Configuring the Nortel VPN Router \(Contivity\)”](#)

Installing and configuring Entrust IdentityGuard

Install the Entrust IdentityGuard 8.0 server. If you want to configure your VPN and RADIUS servers to recognize Entrust IdentityGuard user groups, you must define the groups first. See the *Entrust IdentityGuard Installation and Configuration Guide*.

If you want to display card serial numbers back to the card user during authentication, follow the instructions in the table under “Configuring the Entrust IdentityGuard RADIUS Proxy properties” in the *Technical Integration Guide for Entrust IdentityGuard 8.0 and VPN Router/RADIUS Server*.

You must install the Entrust IdentityGuard RADIUS Proxy and configure it to communicate with your VPN and RADIUS servers before you begin the procedures in this guide. Follow the instructions under “Configuring the Entrust IdentityGuard RADIUS Proxy” in the *Technical Integration Guide for Entrust IdentityGuard 8.0 and VPN Router/RADIUS Server*.

During Entrust IdentityGuard installation, take note of the shared secrets, IP addresses, and ports you used. You need these to configure your VPN and RADIUS servers.

RADIUS Integration overview

Remote Authentication Dial-In User Service (RADIUS) is an industry standard authentication protocol. RADIUS authenticates users through a series of communications between RADIUS clients and the RADIUS server. A RADIUS client passes information about a user to a designated RADIUS server and then acts on the response that the RADIUS server returns. Transactions between the RADIUS client and the RADIUS server are authenticated through a shared secret, which is never sent over the network. Many networks use RADIUS to centralize and coordinate VPN authentication. (For more information on the RADIUS Protocol see RFC 2865, *Remote Authentication Dial in User Service*.)

This integration guide documents how to use the combination of Nortel VPN 3000 Series Concentrator server and the Funk Software Steel-belted RADIUS server with Entrust IdentityGuard. If you are using another RADIUS server, the steps are similar.

If you configure your remote access gateway (IPSec or SSL) to use an existing RADIUS server for configuration, the Entrust IdentityGuard RADIUS Proxy lets you add Entrust IdentityGuard for second factor authentication. The proxy sends the authentication request to the existing RADIUS server to perform primary authentication and then it adds an Entrust IdentityGuard authentication step. Users that do not exist in Entrust IdentityGuard are authenticated by the primary authentication mechanism only.

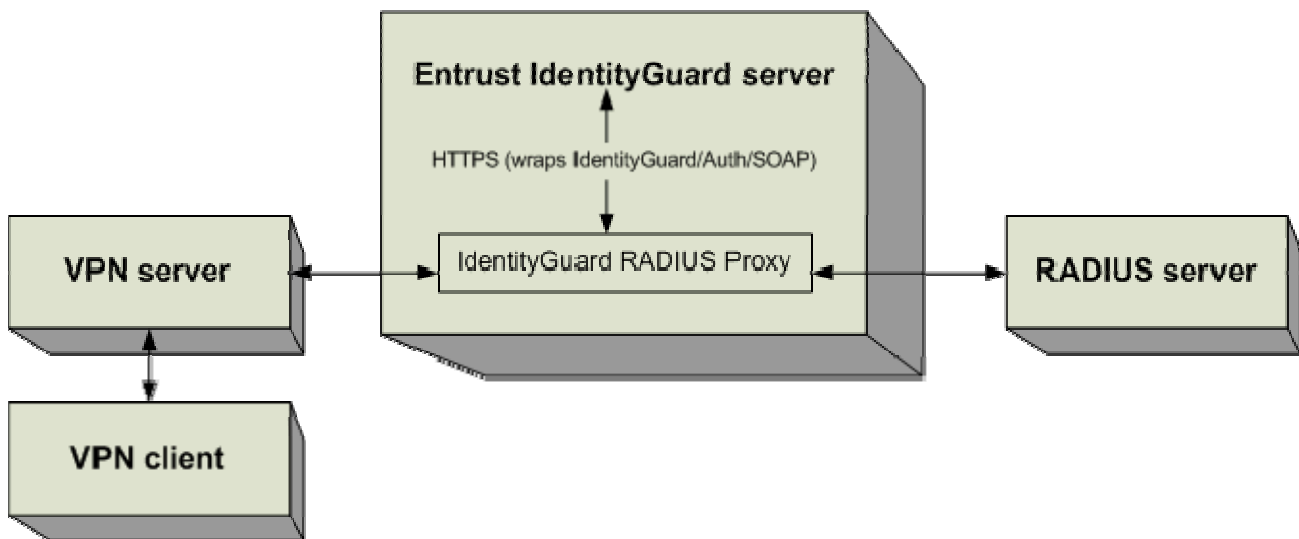
In a normal VPN and RADIUS implementation, the VPN server communicates with the VPN client and with the RADIUS server, while the RADIUS server communicates directly with the VPN server. When you integrate with Entrust IdentityGuard, the Entrust IdentityGuard RADIUS Proxy intercepts messages between the VPN server and RADIUS server, as shown below in Figure 1.

Authentication with Entrust IdentityGuard follows these steps:

1. The VPN server sends an authentication request to the Entrust IdentityGuard RADIUS Proxy.
2. The proxy forwards the request to the RADIUS server.
3. How the RADIUS server responds to the proxy determines the next steps:

- If the RADIUS server sends a reject message, the proxy forwards it unchanged to the VPN server.
 - If the RADIUS server sends an accept message, the proxy keeps the message and requests a challenge from the Entrust IdentityGuard server and sends the challenge to the VPN server (which in turn forwards this to the VPN client). The challenge requires a PIN or a response from a user's card.
4. The VPN server sends the user's response to the challenge back to the proxy.
 5. The proxy forwards the response to the Entrust IdentityGuard server.
 6. The Entrust IdentityGuard server authenticates the response (or not) and the proxy sends an accept or reject message to the VPN server.
 7. An accept message indicates the user has now passed second factor authentication.

Figure 1: Overview of Entrust IdentityGuard 8.0 integrated with a VPN and RADIUS server.



Integration details

The following example use the administration interfaces of the Nortel VPN Router CES1700D (Contivity) and the Funk Software Steel-belted RADIUS server to first configure a RADIUS and VPN server, then to integrate Entrust IdentityGuard with them.

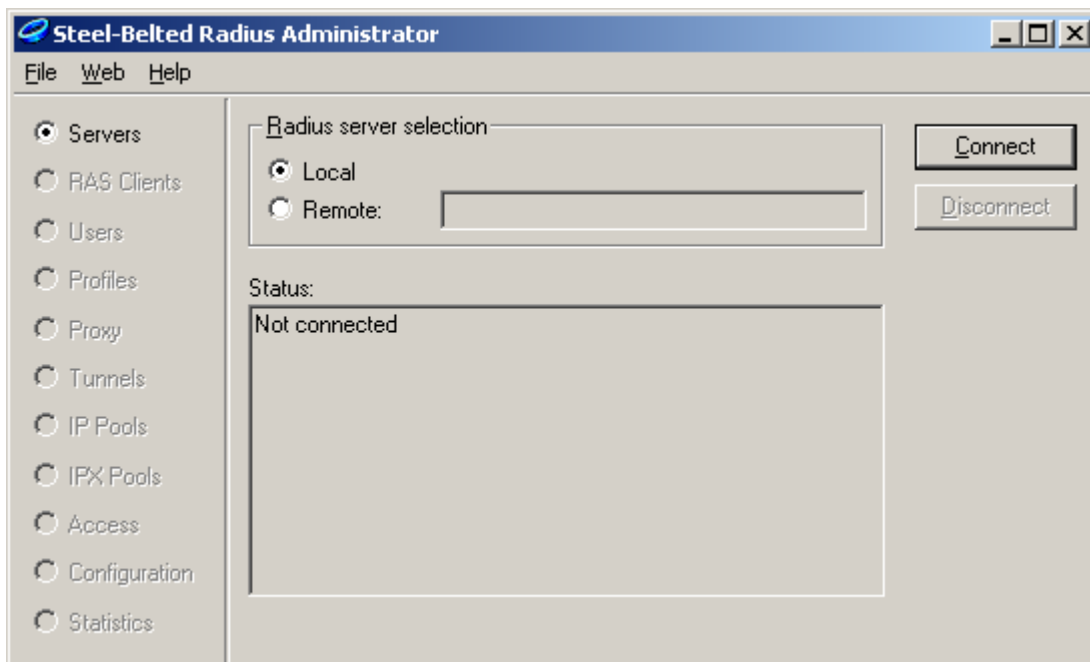
Configuring the RADIUS server

These instructions assume you have already installed Entrust IdentityGuard 8.0 and configured the Entrust IdentityGuard RADIUS Proxy to work with your VPN and RADIUS servers, and you may have associated different groups of users with different RADIUS servers.

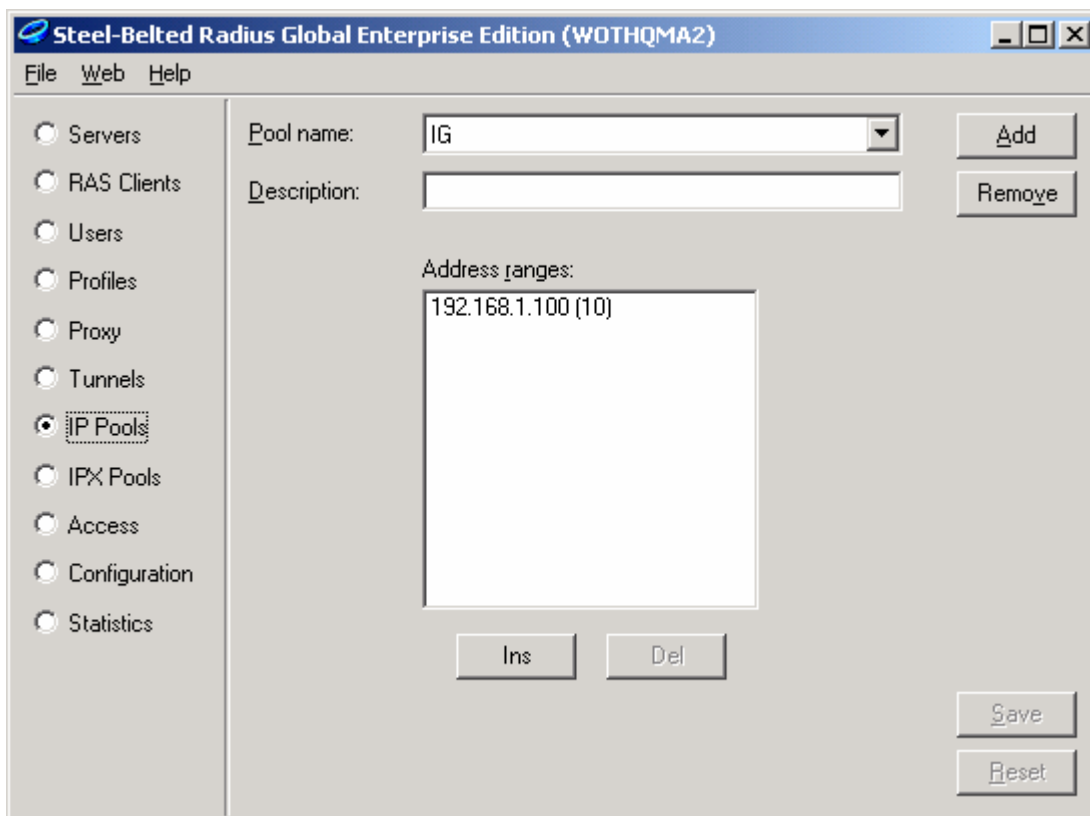
To configure the RADIUS server

These instructions describe how to configure a RADIUS server. Later you can modify your RADIUS configuration to use the Entrust IdentityGuard RADIUS Proxy. (See "[Solution Configuration with Entrust IdentityGuard 8.0.](#)")

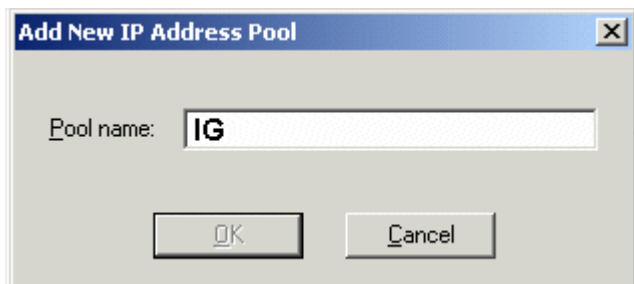
1. Log in to the RADIUS server as administrator. The following window appears.



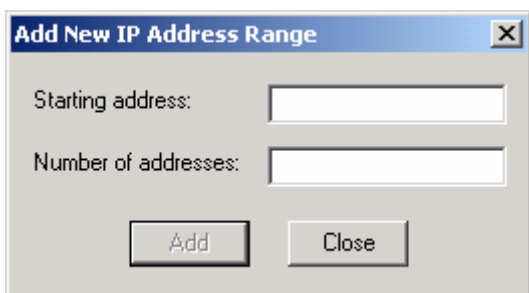
2. Click **Connect**. The following administration window appears.



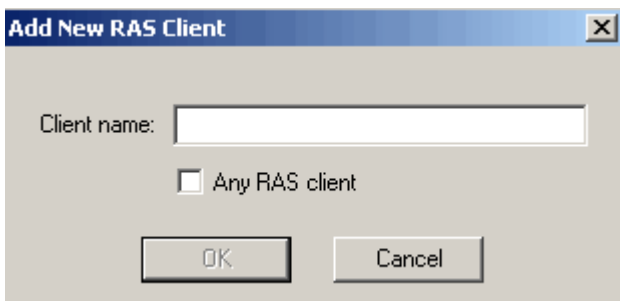
3. To configure the IP Pool, select **IP Pools** in the left-hand options list and click **Add**. The **Add New IP Address Pool** dialog box appears.



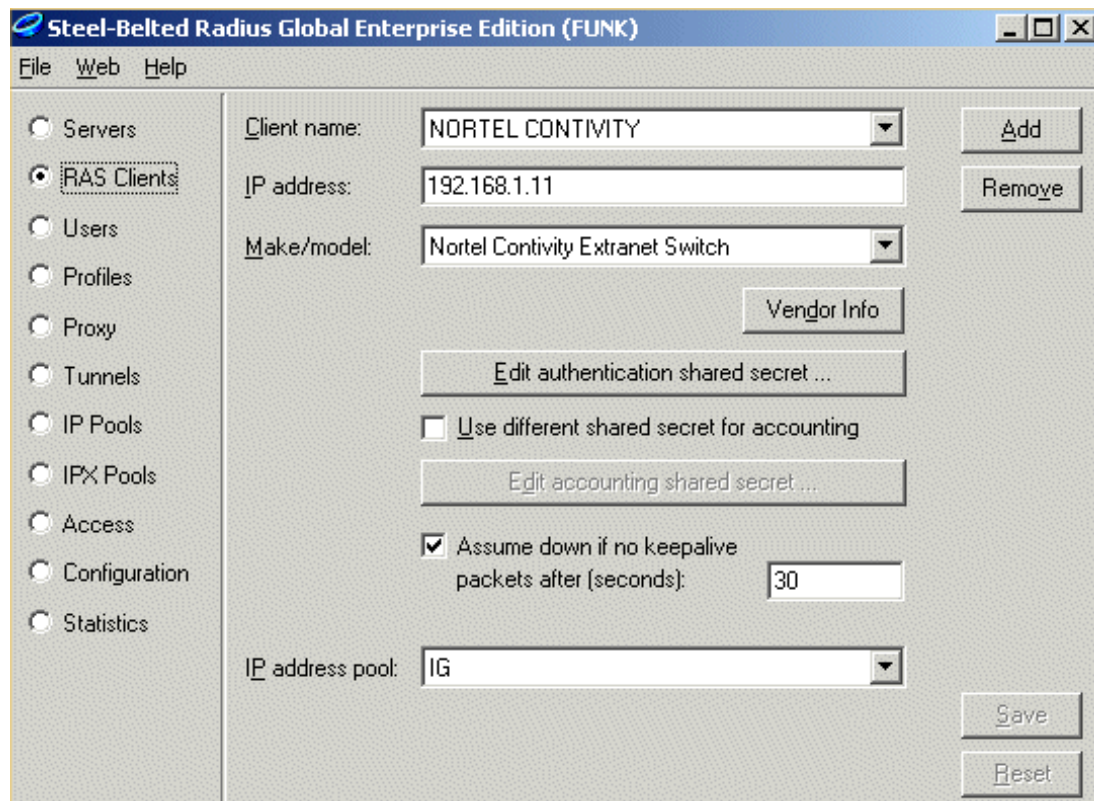
4. Enter the name of the IP address. For this example, use the name **IG**. Click **OK**.
5. In the administration window, click **Ins**. The **Add New IP Address Range** dialog box reappears.



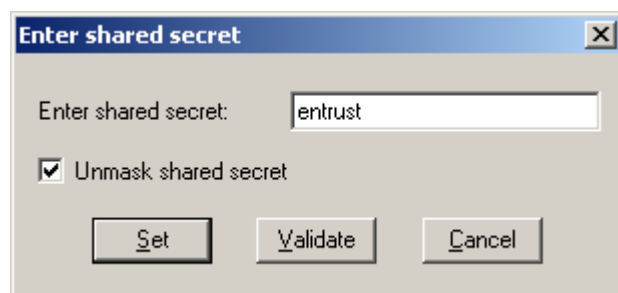
6. Enter a value for **Starting address** and **Number of addresses**. Click **Add**.
7. Next, configure the RAS client. Select **RAS Clients** in the left-hand options list on the administration window.
8. Click **Add**. The **Add New RAS Client** dialog box appears.



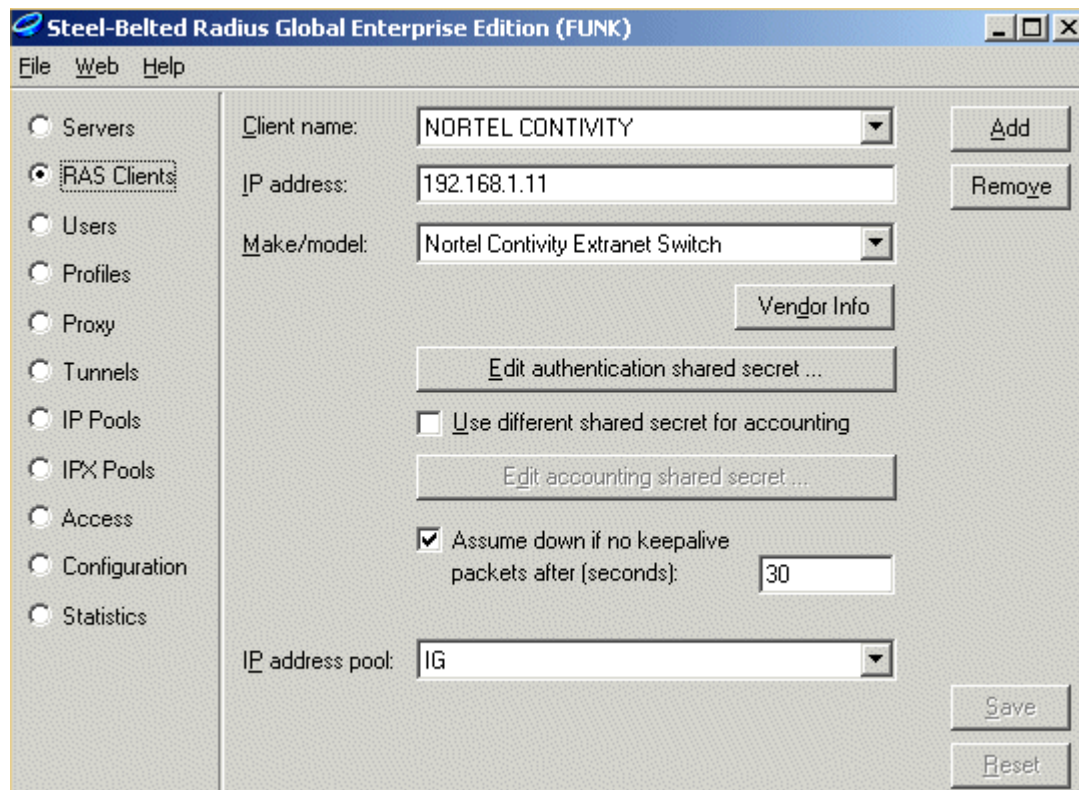
9. Enter a client name for the Nortel VPN Router and click **OK**. The Nortel VPN Router name now appears in the **Client name** field on the administration window.



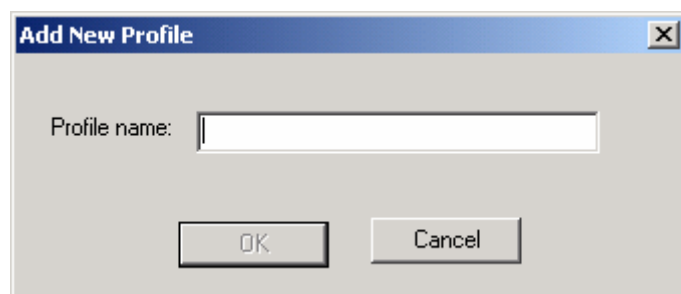
10. In the **IP address** field, enter the IP address for Nortel VPN Router (Contivity).
11. In the **Make/model** field, select **Nortel Contivity Extranet Switch** from the drop-down list.
12. Click **Edit authentication shared secret**. The following dialog box appears.



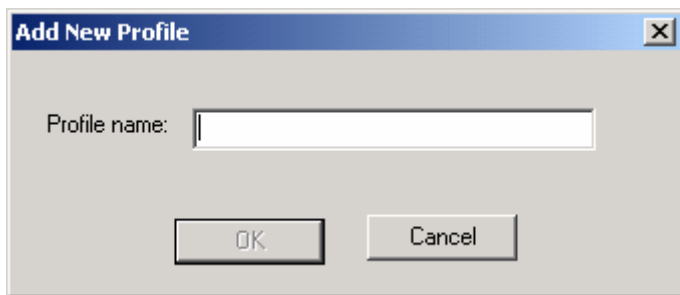
13. Enter the shared secret, and click **Set**.



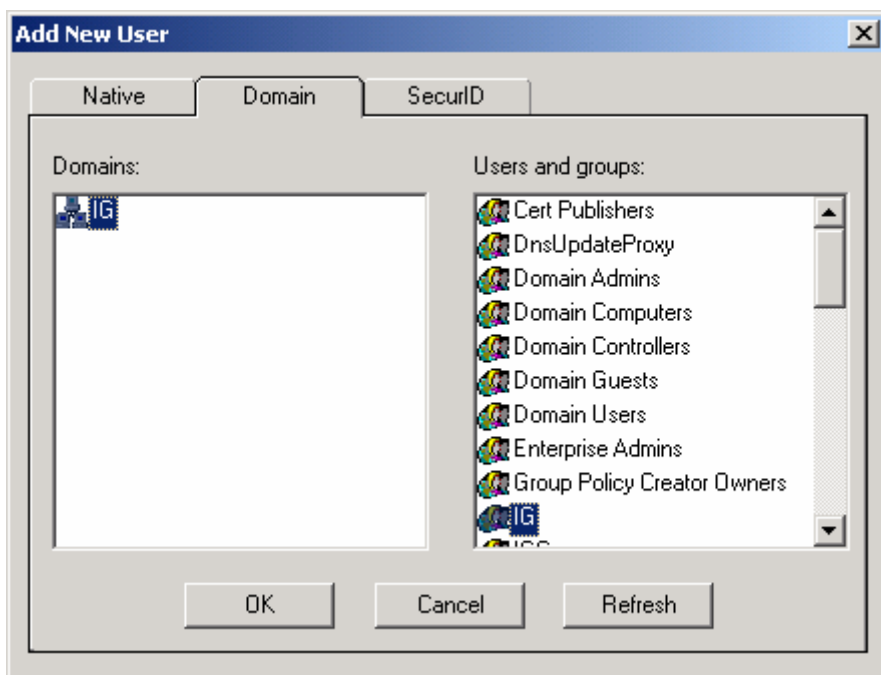
14. In the administration window, select the pool name you set in Step 5 from the **IP address pool** drop-down list.
15. Configure a new profile. In the administration window, select **Profiles** in the left-hand options list and click **Add**. The **Add New Profile** dialog box appears.



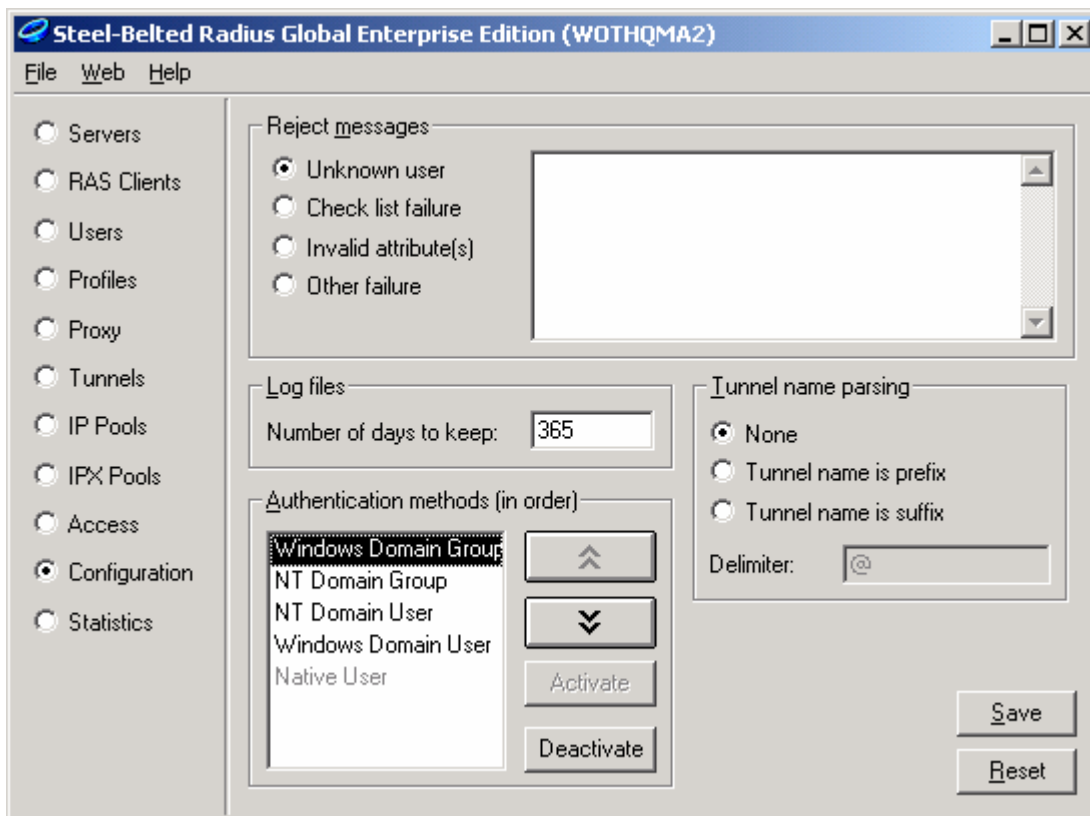
16. Enter the name of the new profile and click **OK**.
17. In the administration window, select **Users** in the left-hand options list to begin configuring user mapping. Click **Add**. The **Add New Profile** dialog box appears.



18. Enter the new user profile name and click **OK**.
19. In the administration window, select **Users** again in the left-hand options list and click **Add**. The **Add New User** dialog box appears.



20. In the left pane, select the domain you want to add the user or group to, and then select the user or group in the right pane. Click **OK**.
21. Map the user group by selecting the target profile (such as IG).



22. Lastly, configure the authentication method. In the administration window, select **Configuration** in the left-hand options list.

23. Under **Authentication methods**, arrange the methods in the correct order using the up and down arrow keys.

24. Click **Save** to save all configurations.

Configuring the Nortel VPN Router (Contivity)

IPSec tunnels require that you establish a secure session before exchanging any data. To establish such a session, a pre-shared key is required. You cannot use the client's user name and password to set up the tunnel since the user ID and password are unknown. (These are stored on the Active Directory, to which the external RADIUS server points.) To overcome this problem, use the Group ID and shared password (configured on both Contivity and the client) to create a secure session.

Contivity can securely pass the user name and password to the authentication server. In this way, Contivity establishes the secure tunnel with the client.

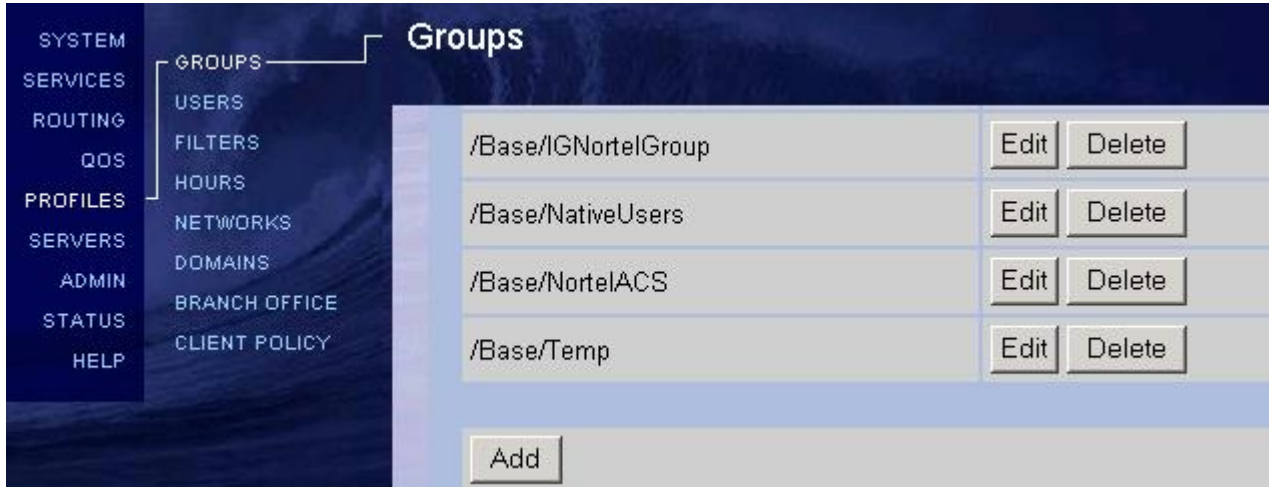
- It uses the Group ID to bind the tunnel to a particular group and the password as a pre-shared key.
- Once the tunnel is established, Contivity verifies the client's user name and password against the external RADIUS server (which points to the Active Directory).
- If RADIUS accepts the authentication, Contivity establishes the tunnel and the user can send and receive data.
- If RADIUS rejects the authentication, Contivity brings the tunnel down.

The following instructions describe how to modify your VPN configuration to use the Entrust IdentityGuard RADIUS Proxy. They assume you have already configured the Entrust IdentityGuard RADIUS Proxy to work with your VPN

and RADIUS servers, and may have associated different groups of users with different RADIUS servers. See the *Technical Integration Guide for Entrust IdentityGuard 8.0 and VPN Router/RADIUS Server* for details.

To configure group authentication

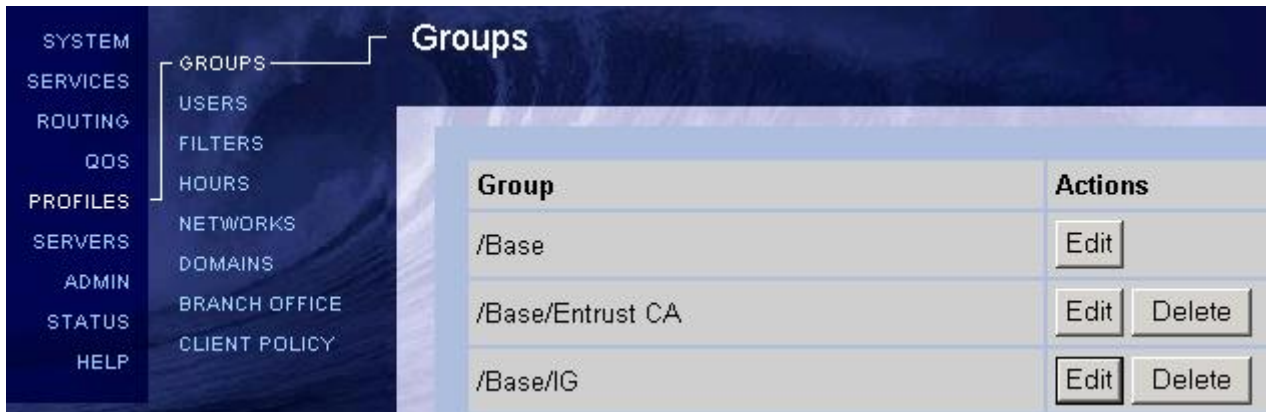
1. Open the Contivity VPN administration interface.



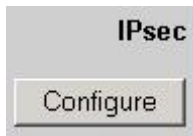
2. In the left-hand pane, select **Profiles > Groups** and click **Add** to add a new VPN group.



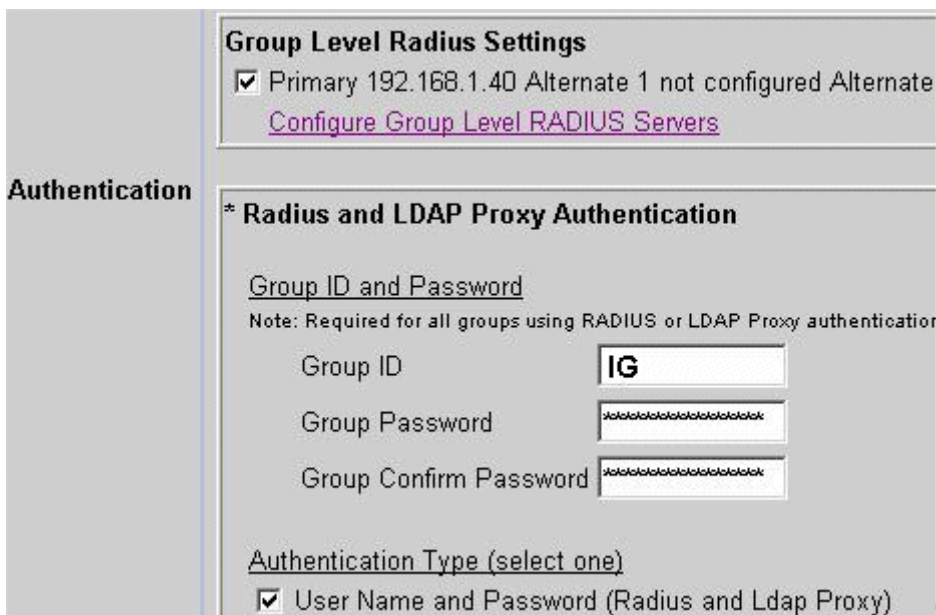
3. Enter a name in the **Group Name** field (for example, IG).
4. Select a parent group in the **Parent Group** drop-down list and click **OK**.



- The previous window appears. Locate the group name you just added (in this case /Base/IG) and click **Edit**.



- Under **IPsec**, click **Configure**.



- Under **Radius and LDAP Proxy Authentication**, enter the group name and group password. Confirm the password.
- Select **User Name and Password** as the authentication type.
- Click **OK** to save the configuration.

To configure the RADIUS server connection

- Open the Contivity administration interface.
- In the left-hand pane, click **Servers > Radius Auth**.

RADIUS Authentication

Enable Access to RADIUS Authentication

Remove Suffix from User ID (e.g. jsmith@nortelnetworks.com) (Does not work with MSCHAPV2)
 Delimiter Value=@

Remove Prefix from User ID (e.g. domain\jsmith) (Does not work with MSCHAPV2)
 Delimiter Value=\

Error Code Pass Thru Enable (optional)

RADIUS Users Obtain Default Settings from the Group /Base/IG

Server-Supported Authentication Options

Enabled	Type	Description
<input type="checkbox"/>	CHALLENGE	Challenge/Response Token Cards
<input type="checkbox"/>	RESPONSE	Response Only Token Cards
<input type="checkbox"/>	MS-CHAP-V2	MSCHAPV2 - Microsoft encrypted CHAP. Version 2
<input type="checkbox"/>	MS-CHAP	MSCHAP - Microsoft encrypted CHAP. Version 1 <input type="checkbox"/> RFC-2548 (Microsoft Vendor-specific RADIUS Attributes) compliant
<input checked="" type="checkbox"/>	CHAP	CHAP - Challenge Handshake Authentication Protocol.
<input checked="" type="checkbox"/>	PAP	PAP - Password Authentication Protocol.

- At the top of the window, select **Enable Access to RADIUS Authentication**.
- In the **RADIUS Users Obtain Default Settings from the Group** drop-down list, select the group you created earlier (for example, /Base/IG).
- Under **Server Supported Authentication Options**, select **Enabled** for the **CHAP** and **PAP** options only.

RADIUS Servers

Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret	Confirm Secret
<input checked="" type="checkbox"/>	Primary	192.168.1.30	<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Configured	1812
<input type="checkbox"/>	Alternate 1		<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Not Configured	1645		
<input type="checkbox"/>	Alternate 2		<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Not Configured	1645		
		Response Timeout Interval	3 (seconds)				
		Maximum Transmit Attempts	3				

- In the **RADIUS Servers** section of the window, do the following:

- Select **Enabled** for the primary server.
 - In the **Host Name or IP Address** field of the primary server, enter the DNS or IP address of the Entrust IdentityGuard RADIUS Proxy.
 - In the **Port** field of the primary server, enter the port number of the RADIUS server where the Entrust IdentityGuard RADIUS Proxy sends requests. (The default Entrust IdentityGuard port is 1812 but this may vary depending on your proxy configurations. See [“To configure multiple groups to work with Entrust IdentityGuard”](#) below.)
 - In the **Secret** and **Confirm Secret** fields, enter and confirm the shared secret for the RADIUS server.
7. Click **OK** to save the configuration.
 8. In the left-hand menu pane, click **Profiles > Groups** and find the group you added earlier.
 9. Under **Actions**, click **Edit**.



10. Under **IPsec**, click **Configure**.



11. Under **Group Level Radius Settings**, select the **Primary** option, and click the **Configure Group Level RADIUS Servers** link. Scroll down to the following section of the window that appears.

RADIUS Servers							
Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret	Confirm Secret
<input checked="" type="checkbox"/>	Primary	192.168.1.30	<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Configured	1812
<input type="checkbox"/>	Alternate 1		<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Not Configured	1645		
<input type="checkbox"/>	Alternate 2		<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Not Configured	1645		
Response Timeout Interval			3 (seconds)				
Maximum Transmit Attempts			3				

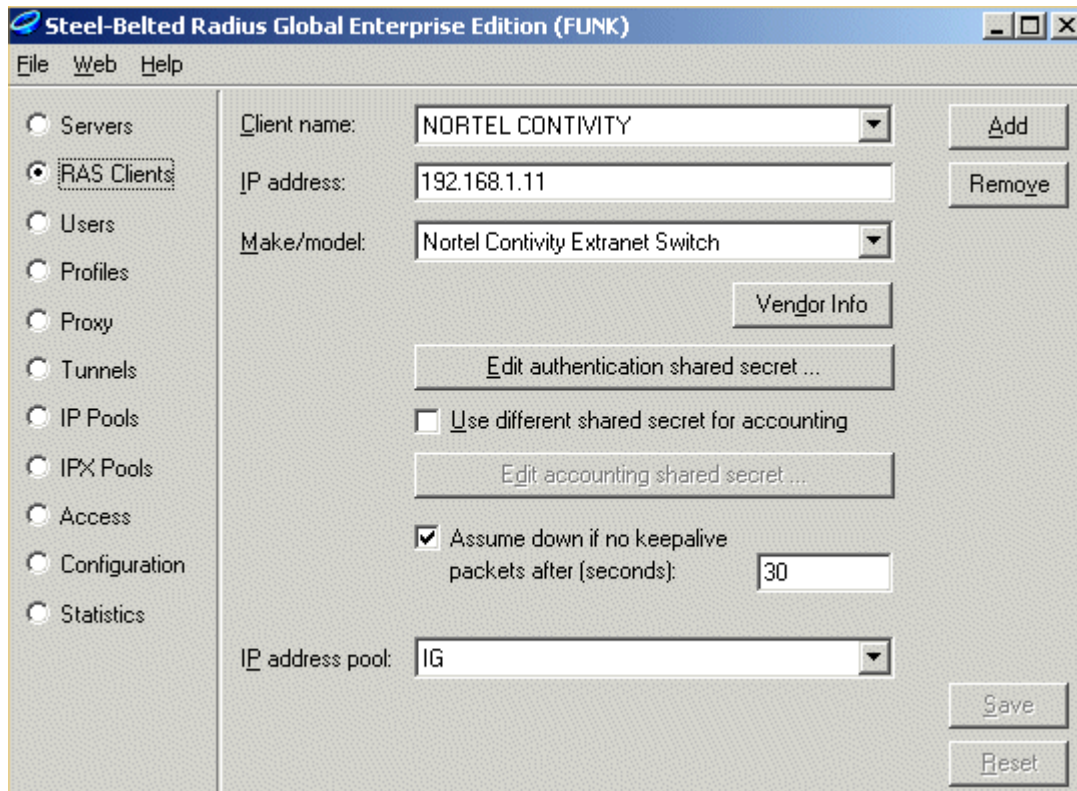
12. Ensure that the RADIUS server information is correct.
13. Click **OK** to save the configuration.

Configuration for Entrust IdentityGuard 8.0

This section explains how to easily configure your RADIUS server and VPN server configurations to use the Entrust IdentityGuard RADIUS Proxy.

To configure the RADIUS connection to Entrust IdentityGuard RADIUS Proxy

1. Start the Funk RADIUS server administrator interface and click **Connect**.
2. From the left-hand options, select **RAS Clients**. The following window appears.



The screenshot shows the 'Steel-Belted RADIUS Global Enterprise Edition (FUNK)' application window. The left-hand navigation pane has 'RAS Clients' selected. The main area displays configuration fields for a client named 'NORTEL CONTIVITY'. The fields include: Client name (dropdown), IP address (192.168.1.11), Make/model (Nortel Contivity Extranet Switch), and IP address pool (IG). There are buttons for 'Add', 'Remove', 'Vendor Info', 'Edit authentication shared secret ...', 'Edit accounting shared secret ...', 'Assume down if no keepalive packets after (seconds): 30', 'Save', and 'Reset'. A checkbox for 'Use different shared secret for accounting' is unchecked.

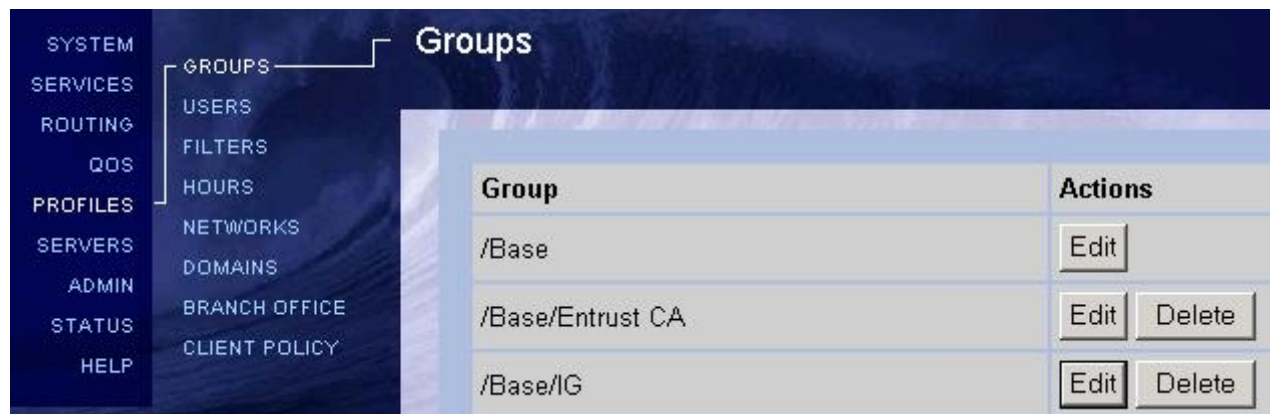
3. In the **Client name** field, select the previously configured client **Nortel Contivity**.
4. Change the **IP address** to point to the Entrust IdentityGuard RADIUS Proxy instead of the Nortel VPN Router.
5. Click **Save** to save the changes.

To configure the VPN connection to Entrust IdentityGuard RADIUS Proxy

1. Open the Contivity administration interface.
2. In the left-hand pane, click **Servers > Radius Auth**.

RADIUS Servers							
Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret	Confirm Secret
<input checked="" type="checkbox"/>	Primary	<input type="text" value="192.168.1.40"/>	<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public <input type="text" value="10.4.121.243"/>	Configured	<input type="text" value="1812"/>	<input type="text" value="*****"/>	<input type="text" value="*****"/>
<input type="checkbox"/>	Alternate 1	<input type="text"/>	<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public <input type="text" value="10.4.121.243"/>	Not Configured	<input type="text" value="1645"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Alternate 2	<input type="text"/>	<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public <input type="text" value="10.4.121.243"/>	Not Configured	<input type="text" value="1645"/>	<input type="text"/>	<input type="text"/>
Response Timeout Interval			<input type="text" value="3"/> (seconds)				
Maximum Transmit Attempts			<input type="text" value="3"/>				

- In the **RADIUS Servers** section of the window, do the following:
 - In the **Host Name or IP Address** field of the primary server, enter the DNS or IP address of the Entrust IdentityGuard RADIUS Proxy.
 - In the **Port** field of the primary server, enter the port number of the RADIUS server where the Entrust IdentityGuard RADIUS Proxy sends requests. (The default Entrust IdentityGuard port is 1812 but this may vary depending on your proxy configurations. See [“To configure multiple groups to work with Entrust IdentityGuard”](#) below.)
 - In the **Secret** and **Confirm Secret** fields, enter and confirm the shared secret for the RADIUS server.
- Click **OK** to save the configuration change.
- In the left-hand pane, select **Profiles > Group** and find the applicable group (for example, /Base/IG).



- Under Actions, click **Edit**.



7. Under IPsec, click **Configure**.

Group Level Radius Settings

Primary 192.168.1.40 Alternate 1 not configured Alternate 2 not configured

[Configure Group Level RADIUS Servers](#)

8. Under **Group Level Radius Settings**, select Primary and click the **Configure Group Level RADIUS Servers** link. Scroll down to the following section of the window that appears.

RADIUS Servers							
Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret	Confirm Secret
<input checked="" type="checkbox"/>	Primary	192.168.1.40	<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Configured	1812	*****	*****
<input type="checkbox"/>	Alternate 1		<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Not Configured	1645		
<input type="checkbox"/>	Alternate 2		<input checked="" type="radio"/> Private (192.168.1.11) <input type="radio"/> Public 10.4.121.243	Not Configured	1645		
Response Timeout Interval			3 (seconds)				
Maximum Transmit Attempts			3				

9. Ensure that the RADIUS server information is correct.

10. Click **OK** to save the configuration.

To configure multiple groups to work with Entrust IdentityGuard

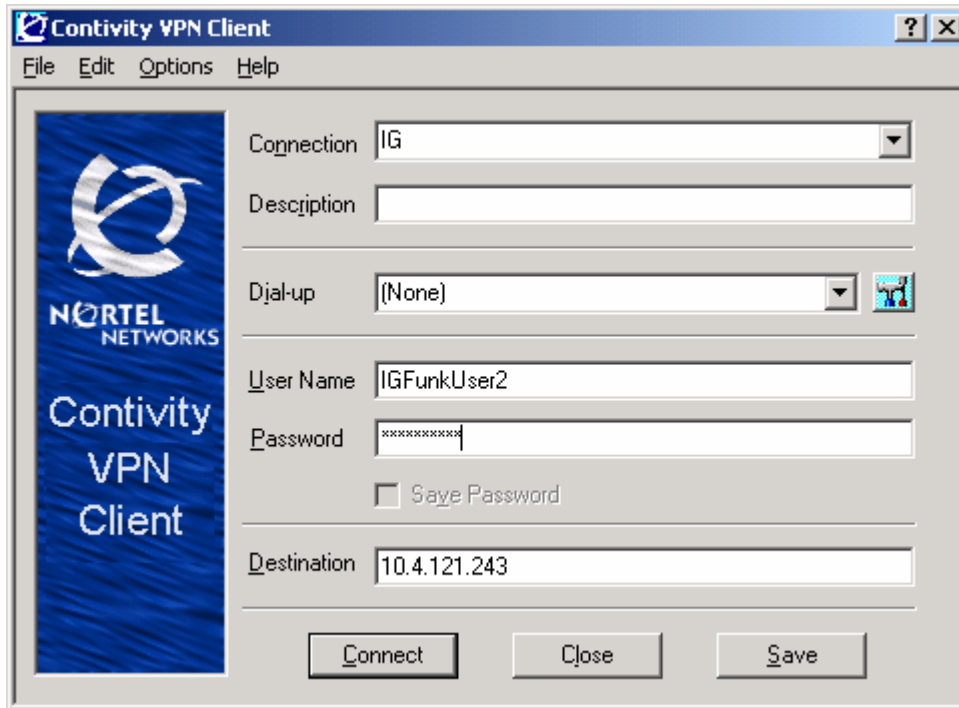
You can take advantage of the Entrust IdentityGuard multiple groups feature to organize users into different groups for authentication purposes. For example, assume you have already defined two groups of users in Entrust IdentityGuard and have already configured the Entrust IdentityGuard RADIUS Proxy to associate those groups with specific RADIUS ports (for example, 1812 and 1813).

In a previous section, you created a VPN server configuration for a group named IG that uses RADIUS port 1812. Follow the same steps to create a VPN server configuration for another group. But, when it comes to setting a RADIUS port, enter the port number (such as 1813) you assigned to the second group when you configured the Entrust IdentityGuard RADIUS Proxy.

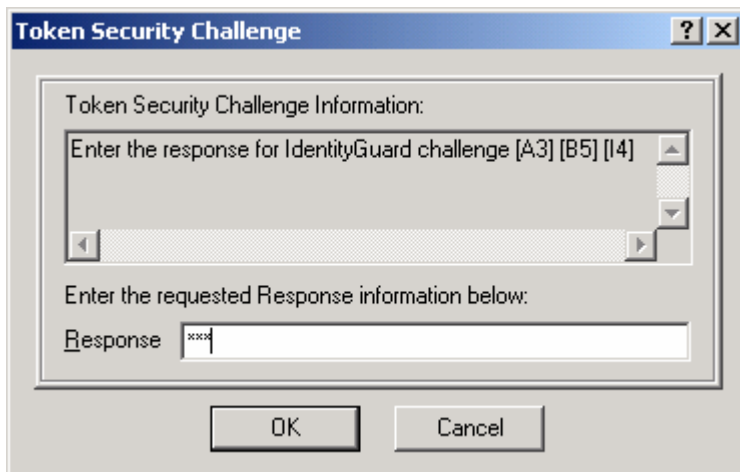
The VPN group names and the group names specified in the Entrust IdentityGuard RADIUS Proxy do not have to match (though matching names may be less confusing). You associate VPN server groups with Entrust IdentityGuard groups using a specific RADIUS server port number.

Testing the configuration with Entrust IdentityGuard 8.0

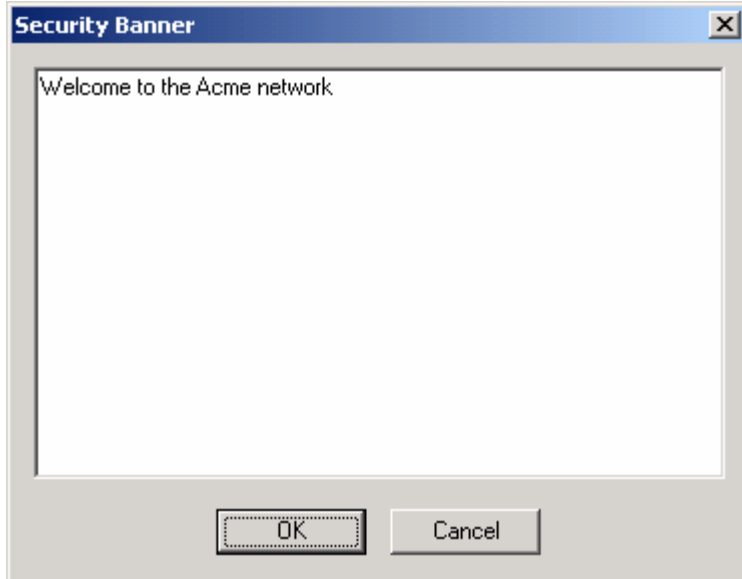
1. Start the Contivity VPN Client.



2. In the Contivity VPN Client dialog box, enter the user name and password and click **Connect**. If the configuration is correctly set up, the Entrust IdentityGuard **Token Security Challenge** dialog box appears.



3. Enter the challenge response in the **Response** field as a string without spaces or punctuation and click **OK**.



4. When the **Security Banner** dialog box appears, click **OK**.



5. If the above dialog box appears, it confirms the connection is set properly. Click **OK**.

Once you complete and test the configuration of your VPN and RADIUS servers as described above, your system is integrated to work with Entrust Identity Guard. You can configure other VPN and RADIUS servers as needed.