Avaya VPN Router Configuration – Client

Avaya VPN Router
Release 8.01

Document Status: **Standard**

Document Number: **NN46110-306**

Document Version: **03.01**

Date: **December 2010**

© 2010 Avaya Inc. All Rights Reserved.

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- "Getting technical documentation" on page 7
- "Getting product training" on page 7
- "Getting help from a distributor or reseller" on page 8
- "Getting technical support from the Avaya Web site" on page 8

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Preface

This guide provides information to configure the Avaya VPN Client. Topics include:

- creating profiles using various authentication methods
- configuring optional application settings
- controlling the client from a script or a third-party application

This guide is for network managers who configure client software for the VPN Router. This guide assumes that you have the following background:

- experience with Windows-based systems or graphical user interfaces (GUI)
- familiarity with network management

For information about how to install or upgrade the Avaya VPN Client, see *Avaya VPN Router Installation and Upgrade — Client Software Release 8.01* (NN46110-409).

Before you begin

The minimum PC requirements to run the Avaya VPN Client are:

- Windows 2000 or Windows XP
- 200 megahertz (MHz) Pentium
- 64 megabyte (MB) memory
- 10 MB free hard disk space

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **ping** <*ip_address*>, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off | on**}.
braces ({})	Indicate required elements in syntax descriptions where more than one option exists. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **ldap-server source {external | internal}**, you must enter either **ldap-server source external** or **ldap-server source internal**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **show ntp [associations]**, you can enter either **show ntp** or **show ntp associations**. Example: If the command syntax is **default rsvp** [**token-bucket** {**depth | rate**}], you can enter **default rsvp**, **default rsvp token-bucket depth**, or **default rsvp token-bucket rate**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **more disk***n*:<*directory*>**/...**<*file_name*>, you enter **more** and the fully qualified name of the file.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore (_). Example: If the command syntax is **`ping`** <*`ip_address`*>, *`ip_address`* is one variable, and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`
separator (,)	Shows menu paths. Example: Select Status, Health Check.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **`terminal paging`** {**`off | on`**}, you enter either **`terminal paging off`** or **`terminal paging on`**, but not both.

Related publications

For more information about the Avaya VPN Client, see the following publications:

- Release notes provide the most recent information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Avaya VPN Client Configuration — TunnelGuard* (NN46110-307) provides information to configure and use the TunnelGuard feature.
- *Avaya VPN Router Upgrades — Server Software Release 8.0* (NN46110-407) provides information to upgrade the server software to the most recent release.
- *Avaya VPN Router Installation and Upgrade — Client Software Release 8.01* (NN46110-409) provides information to upgrade the Avaya VPN Client to the most recent release.
- *Avaya VPN Client Configuration — Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *Avaya VPN Client Configuration — SSL VPN Services* (NN46110-501) provides instructions to configure services on the SSL VPN Module 1000, including authentication, networks, user groups, and portal links.
- *Avaya VPN Router Configuration — Advanced Features* (NN46110-502) provides configuration information for advanced features such as the Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other vendors.
- *Avaya VPN Client Configuration — Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F).
- *Avaya VPN Client Configuration — Routing* (NN46110-504) provides instructions to configure the Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy services, and client address redistribution (CAR).
- *Avaya VPN Client Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface (CLI).

- *Avaya VPN Client Configuration — Firewalls, Filters, NAT, and QoS* (NN46110-508) provides instructions to configure the Stateful Firewall and VPN Client interface and tunnel filters.
- *Avaya VPN Client Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.
- *Avaya VPN Client Troubleshooting — Server* (NN46110-602) provides information about system administrator tasks such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.
- *Avaya VPN Router Administration* (NN46110-603) provides information about system administrator tasks such as backups, file management, serial connections, initial passwords, and general network management functions.
- *Avaya VPN Client Troubleshooting — Client* (NN46110-700) provides information to troubleshoot installation and connectivity problems with the Avaya VPN Client.

Hard-copy technical manuals

To print selected technical manuals and release notes free, directly from the Internet, go to www.avaya.com/support. Find the product for which you need documentation, and then locate the specific category and model or version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and then print them on most standard printers. Go to the Adobe Systems Web site at www.adobe.com to download a free copy of the Adobe Reader.

New in this release

The following sections details what’s new in *Avaya VPN Router Configuration — Client* (NN46110-306) for Release 8.01:

- “Features” on page 15
- “Other changes” on page 15

Features

See the following sections for information about feature changes:

- “PassGo” on page 15
- “Two factor authentication” on page 15

PassGo

Release 8.01 supports PassGo tokens for authentication. For more information, see “Appendix A” on page 61.

Two factor authentication

Release 8.01 supports two factor authentication for VPN Router Release 8.0. For more information, see “Two factor authentication” on page 40.

Other changes

See the following sections for information about changes that are not feature-related:

- “Removed content” on page 16

Removed content

Information about how to install or upgrade the Avaya VPN Client is moved to *Avaya VPN Router Installation and Upgrade — Client Software Release 8.01* (NN46110-409).

Information about client releases that Avaya no longer supports is removed.

Chapter 1
Avaya VPN Client

This chapter provides information about how to use Avaya VPN Client, including authentication methods, Windows domain logon, tunneling modes, and security banners.

Avaya VPN Client supports dynamic Domain Name System (DNS) registration, which you configure at the group level on VPN Router. Avaya VPN Client also provides support for IP security (IPsec) mobility, and persistent tunneling.

The following table shows the versions of the client available in limited (56-bit) or full (128-bit) form, as well as the available encryption methods, Diffie-Hellman groups, and hashes.

Table 1 Avaya VPN Client support

Version	56-bit	128-bit	256-bit	Diffie Hellman groups	Hash
5.11 (FIPS)	NA	3DES, AES-128	AES-256	2, 5, 8	SHA-1
6.01	NA	DES (40, 56), 3DES, AES-128	AES-256	1, 2, 5, 8	MD5, SHA-1
6.02 (translated)	NA	DES (40, 56) 3DES, AES-128	AES-256	1, 2, 5, 8	MD5, SHA-1
7.01	NA	DES (40, 56) 3DES, AES-128	AES-256	1, 2, 5, 8	MD5, SHA-1
8.01	NA	DES (40, 56) 3DES, AES-128	AES-256	1, 2, 5, 8	MD5, SHA-1

This chapter includes the following topics:

- "Windows domain logon" on page 41
- "Application launch" on page 46
- "Optimizing the TCP window" on page 47
- "Banners" on page 48
- "Tunneling modes" on page 51
- "IPsec mobility and persistence" on page 51
- "Coexisting with Microsoft IPsec Service" on page 52

Using the Avaya VPN Client for the first time

The following procedures explain how to configure the first VPN connection.

Configuring a user name and password connection

Start the Avaya VPN Client and use a user name and password.

1. Choose **Start**, **All Programs**, **Avaya**, **Avaya VPN Client**, **Avaya VPN Client**.

   The Connection Wizard window appears.

2. Click **Yes** if you want to use the Connection Wizard to create the first connection.

   The New Connection Profile window appears.

   OR

   Click **No** if you want to manually provide the information.

3. Type a name for the connection profile. You can optionally type a description of the profile.
4. Click **Next**.

   The Authentication Type window appears.

5 Select **Username and Password**.

6 Click **Next**.

The User Identification window appears.

7 Type the user name and password. If you want to save the password, select **Save the Password**.

8 Click **Next**.

The Group Authentication Information window appears.

9 Click **Yes** if you use a group ID and group password.

OR

Click **No** if you do not have a group ID and group password.

10 Click **Next**.

The Destination window appears.

11 Type either the host name or the IP address of the VPN Router at the remote network.

12 Click **Next**.

The Dial-up Connection window appears.

13 Select **No** if you do not want to dial first.

OR

Select **Yes** if you want to establish a dial-up connection before the VPN connection.

14 Click **Next**.

The Connection Profile Complete window appears.

15 Click **Finish**.

Configuring a hardware or software token connection

Start the Avaya VPN Client and use a hardware or software token.

1 Choose **Start**, **All Programs**, **Avaya**, **Avaya VPN Client**, **Avaya VPN Client**.

The Connection Wizard window appears.

2 Click **Yes** if you want to use the Connection Wizard to create the first connection.

The New Connection Profile window appears.

OR

Click **No** if you want to manually provide the information.

3 Type a name for the connection profile. You can optionally type a description of the profile.

4 Click **Next**.

The Authentication Type window appears.

5 Select **Hardware or Software Token Card**.

6 Click **Next**.

The User Token Card window appears.

7 Select the type of token you want to use.

8 Click **Next**.

The Token Group Information window appears.

9 Type the user and group token information.

10 Click **Next**.

The Destination window appears.

11 Type either the host name or the IP address of the VPN Router at the remote network.

12 Click **Next**.

The Dial-up Connection window appears.

13 Select **No** if you do not want to dial first.

OR

Select **Yes** if you want to make a dial-up connection first.

14 Click **Next**.

The Connection Profile Complete window appears.

15 Click **Finish**.

Configuring a certificate and smartcard connection

Start the Avaya VPN Client and use a digital certificate and smartcard.

1 Choose **Start**, **All Programs**, **Avaya**, **Avaya VPN Client**, **Avaya VPN Client**.

The Connection Wizard window appears.

2 Click **Yes** if you want to use the Connection Wizard to create the first connection.

The New Connection Profile window appears.

OR

Click **No** if you want to manually provide the information.

3 Type a name for the connection profile. You can optionally type a description of the profile.

4 Click **Next**.

The Authentication Type window appears.

5 Select **Digital Certificate and Smartcard**.

6 Click **Next**.

The Digital Certificate Type window appears.

7 Select the type of certificate you want to use.

8 Click **Next**.

9 Select the certificate.

10 Click **OK**.

The Destination window appears.

11 Type either the host name or the IP address of the VPN Router at the remote network.

12 Click **Next**.

The Dial-up Connection window appears.

13 Select **No** if you do not want to dial first.

OR

Select **Yes** if you want to make a dial-up connection first.

14 Click **Next**.

The Connection Profile Complete window appears.

15 Click **Finish**.

Authentication methods

This section provides information about how to customize the client with the following authentication methods:

- "User name and password" on page 23
- "Digital certificates" on page 23
- "Two factor authentication" on page 40
- "Group security" on page 41

User name and password

When you create a new profile in the client, the default authentication method is the user name and password. With this method, you supply only a user name and password to connect to VPN Router.

Digital certificates

You can use the following two types of digital certificate stores for certificate authentication:

- Microsoft CryptoAPI
- Entrust

Microsoft CryptoAPI

The Avaya VPN Client supports the retrieval of X.509v3 certificates from Microsoft certificate storage through the Microsoft CryptoAPI (MS CAPI). Microsoft provides a public key infrastructure (PKI) that adheres to the Public-Key Cryptography Standards (PKCS).

Microsoft certificate storage provides the Avaya VPN Client full access to the Microsoft certificate storage and management tools. The Microsoft certificate storage and management tools use PKCS standards-based messages and protocols to manage key pair generation and storage.

Microsoft certificate storage uses standard messages (PKCS #12) to import digital certificates granted by third-party certification authorities. Avaya VPN Client and the VPN Router can use certification authorities that do not tightly integrate with the Avaya VPN Client and the VPN Router, for example, Netscape.

The VPN Router Internet Security Association and Key Management Protocol (ISAKMP) supports digital certificates. You can configure both the Avaya VPN Client and the VPN Router to mutually authenticate using digital certificates during the Internet Key Exchange (IKE) negotiation.

➡ **Note:** You can create certificate requests with tools that a certification authority (CA) supports and that integrate with MS CAPI.

MS CAPI server CRL checking

MS CAPI on the Avaya VPN Client supports checking the revocation status of the server certificate. If you receive the following message, this indicates that the server certificate is revoked or the certificate revocation list (CRL) distribution point is inaccessible, as defined in the CRL distribution point extension of the servers X.509 certificate: `The Server's Certificate has been revoked, or could not be validated. Please check with your remote access administrator. The Connection has been terminated.`

Make sure that the CRL distribution point is accessible to the PC after the client tunnel connection is complete. The client must reach the CRL distribution point. An example CRL distribution point, as defined from the issuing CA, is http://sf1.certificates.com/CertEnroll/SF1.crl.

MS CAPI server CRL checking is disabled by default. The registry key at HKLM\Software\Avaya\Avaya VPN Client\MSCAPIServerCRLCheck governs MS CAPI server CRL checking. If the parameter MSCAPIServerCRLCheck is 1, server CRL checking is performed. If the parameter is 0 or missing, server CRL checking is not performed.

Microsoft CA digital certificate request and receipt

Two methods to request and retrieve a digital certificate from the Microsoft CA are the following:

- The trusted CA system creates a digital certificate and distributes it through PKCS #12 bit error rate (BER) encoded messages or files.
- The client system requests a digital certificate, if the trusted CA is accessible from the client that makes the request, by using Microsoft Internet Explorer.

The steps to create the actual digital certificate request (PKCS #10) are always the same, regardless of how you make the request. The difference between the request methods is where the private key material is created and, more importantly, stored.

If you request a digital certificate from the system that houses the Microsoft CA, the CA generates the private key material and stores it locally. The CA generates a PKCS #12 message that is a password-protected, BER-encoded message. The resulting PKCS #12 message contains public and private key material and the associated digital certificate. The CA then distributes the PKCS #12 message to certificate holders in a secure manner and imports it into the MS CAPI store on the local client system.

If you make a digital certificate request from the client, the client generates the private key material and stores it locally. The PKCS #10 message does not contain private key material. Generally, a user wants to keep all private key information and key material private and protected. The client retrieves the digital certificate as a PKCS #7 message and imports it into the MS CAPI store through the Internet Explorer browser or the Internet options CertMgr tool.

To make a request for, and import, a certificate from a browser that runs on the client system or CA system, do the following:

1. Connect to the CA through a Web browser.
2. Select **Request a certificate**.
3. Select **Advanced request**.
4. Select **Submit a certificate request to this CA using a form**.
5. Type the identifying information (Subject distinguished name [DN]).
6. Type the intended purpose (Client Authentication Certificate and IPsec Certificate).

   The Cryptographic Service Provider (CSP) generates the key pair.

7. Click **Submit**.

   Remember the request ID.

Digital certificate import

Two scenarios to import a digital certificate into the MS CAPI store are the following:

- If you use the Microsoft CA, you can import the digital certificate directly from Internet Explorer after you retrieve it from the CA.

- If you use other CA certificates, you or the CA administrator must also produce a PKCS #12 message that contains the private and public key pair and the digital certificate. Then, you can import the key pair and the certificate into the MS CAPI store through the Internet Options tools or the Internet Explorer browser.

Note: When you import a certificate into the MS CAPI store, you must also import the issuing CA certificate.

Microsoft CA digital certificate retrieval

After the Microsoft CA administrator approves the certificate, you can retrieve it through the Internet Explorer browser and import it directly into the MS CAPI store.

Note: You cannot use the Netscape browser because it does not recognize the approved certificates.

1. Connect to the CA from a Web browser.
2. Select **Check on a pending certificate (next ->)**.
3. Select the desired certificate request (**PKCS #7**).
4. To import the PKCS #7 request into the MS CAPI store, select **Certificate Issued - install this certificate?**

   The message `Certificate Installed` appears.

Configuring the Avaya VPN Client for Microsoft stored certificates

You can use the Connection Wizard from the Avaya VPN Client to configure the client connection to use Microsoft stored certificates. You can also configure Microsoft stored certificates by choosing Options, Authentication from the client menu bar.

1. Double-click the **VPN Client** icon.
2. Choose **File**, **Connection Wizard**.
3. Type a name and description.

4. Click **Next**.
5. Select **Digital Certificate and Smartcard**.
6. Click **Next**.
7. Select **Microsoft Stored Certificate**.
8. Click **Next**.

   The Microsoft Certificate Store window appears. By default, this window lists all of the available certificates, including the key usage field for the certificate. If you select Display Only Signature Certificate, only the digital signature appears.

9. Select a certificate.
10. Click **OK**.

Entrust certificate-based authentication

The following sections describe Entrust certificate activities related to the client.

Using a single logon

The Avaya VPN Client supports Entrust Version 6.0 for Entrust single logon. Use the single logon feature to automatically authenticate to all certificate-enabled applications with a single access to your certificate (either an .epf or .tkn file) during a logon session. If you already presented the certificate to authenticate one application, the system does not prompt you to present the certificate for other applications during the logon session.

To use single logon

1. Install Avaya VPN Client as an application.
2. Configure the VPN Router for an Entrust user.
3. Install the Entrust Entelligent Client.
4. Double-click the **Entrust** icon.
5. Log on to the Entrust Entelligent Client.
6. Create an Entrust profile on the Avaya VPN Client.

   The password field appears dimmed on the Avaya VPN Client because the user is logged on.

7. Click **Connect** to establish VPN connection.

Custom installation

You do not need to perform this configuration if you install the Entrust Entelligence software version 4.0 or later.

You can customize the IPsec client to allow remote users to generate new certificates through the client. To create an IPsec client installation that also installs the necessary Entrust components to perform Entrust certificate-based authentication, you must include the following two files in the Client\Custom directory, as you do for custom icon files:

- The Entrust Dynamic Link Libraries (DLL), which are on the Avaya VPN Client CD in the Client\Entrust directory. The Entrust DLLs are kmpapi32.dll and enterr.dll.
- The Entrust .ini file (entrust.ini), which you create when you configure the Entrust PKI server.

Use the Entrust error messages DLL file, enterr.dll, to see more detailed Entrust error messages and information. You can find solutions to many of these error situations through the Entrust knowledge base at www.entrust.com. You need a valid support contract to register and access the knowledge base. The Entrust error messages DLL, enterr.dll, and the Entrust knowledge base can help you resolve many Entrust error situations.

Entrust passwords must conform with the following rules:

- must be at least eight characters in length
- must contain an uppercase character
- must contain a lowercase character
- must contain a numeric character
- must not contain a portion of the profile name longer than half its length
- must not repeat a character more than half the length of the password

Entrust certificate enrollment

Remote users can access an Entrust PKI server to obtain a certificate for tunnel authentication in the following situations:

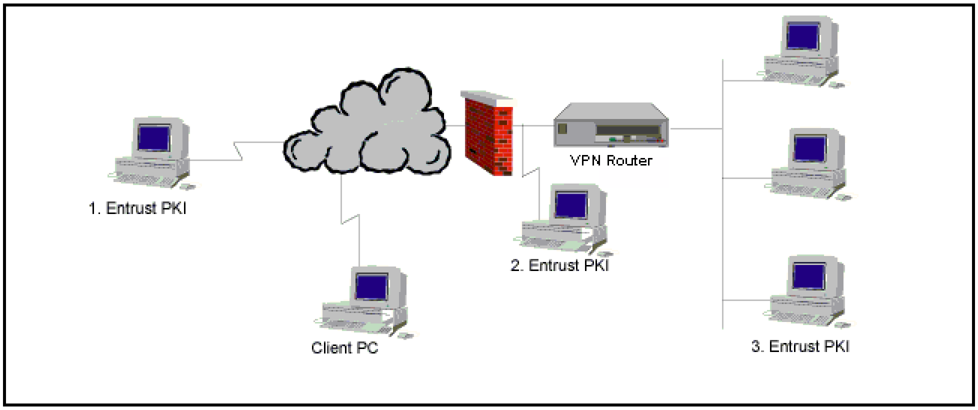
- The external PKI server is accessible from the Internet (directly accessible).
- The PKI server is behind the firewall, but in front of the VPN Router. The firewall must allow ports 389 and 709 to access the PKI (directly accessible).
- The PKI server is behind the firewall and the VPN Router (not directly accessible).

The first two situations are similar because the PKI server is in front of the VPN Router and it is directly accessible from the Internet. When you provide access to the PKI through the firewall from ports 389 and 709, the second situation is the same as the first. The third situation requires remote users to also have a Lightweight Directory Access Protocol (LDAP) user name and password so that a temporary tunnel establishes to access the PKI.

Note: The Entrust tool kit settings determine the protocol and port number used for certificate enrollment. For more information about the ports that you must open on the firewall, see the Entrust documentation.

"Placement options for an Entrust PKI server" on page 30 shows the Entrust PKI server placed in each of the three situations.

Figure 1 Placement options for an Entrust PKI server



Entrust certificate enrollment tunnel

To facilitate Entrust certificate enrollment from an IPsec client that does not directly connect to the Entrust PKI, you must create a special group. Use this group only to access the Entrust PKI to generate a new certificate. You must apply a filter to this group that restricts access through the tunnel to the PKI only. You can name this group, for example, Certificate Enrollment. Add a user with a common user ID and password, for example:

```
User ID: enrollee
Password: certificate
```

You must configure the VPN Router with the correct filters to permit only PKI access through the tunnel filter set and the firewall to the PKI server. The Transmission Control Protocol (TCP) firewall filter ports are 389 and 709. Avaya provides a preconfigured filter rule called Entrust PKI that permits access to the Entrust PKI server. Select this filter for a group from the Profiles, Groups, Edit, Connectivity, Configure menu path. Configure this filter with a deny all filter on the semipublic account that you create. The Entrust PKI filter includes the following rules, and the administrator can customize them if the default Entrust port values are not used:

- TCP, src port > 1023, dest port 389, in
- TCP, src port 389, dest port > 1023, out
- TCP, src port > 1023, dest port 709, in
- TCP, src port 709, dest port > 1023, out

Obtaining a certificate directly from the Internet

Obtain an authentication certificate remotely when the PKI server is directly accessible from the Internet.

1. Choose a directory in which to store the .epf file.
2. Name the **.**epf file.
3. Select a password.
4. Type the values in the **Entrust Reference Number** and **Authorization Code** boxes (obtained from the network administrator).
5. If you use a PKI server behind the firewall and the VPN Router, type the LDAP user name and password, and the IP address or host name of the VPN Router.
6. Choose whether to dial in automatically.
7. Click **Finish**.

Obtaining an Entrust certificate when the Entrust PKI server is behind the firewall and in front of the VPN Router

Obtain a certificate when the Entrust PKI server is behind the firewall and in front of the VPN Router.

1. Double-click the **VPN Client** icon.
2. Choose **File**, **Connection Wizard**.
3. Type a name and description.
4. Click **Next**.

   The Authentication Type window appears.

5. Select **Digital Certificate and Smartcard**.
6. Click **Next**.

   The Digital Certificate Type window appears.

7. Select **Entrust Digital Certificate**.
8. Click **Next**.

The Entrust Certificate Profile Selection window appears.

9 Click **Create a new Profile**.

10 Click **Next**.

The Create Entrust Profile window appears.

11 Follow the prompts to indicate where you want to store the Entrust Profile.

12 Click **Next**.

The Entrust Profile Name window appears.

13 Type a profile name (the name of the local .epf file—do not include the .epf extension) and password.

14 Click **Next**.

The Reference Number and Authorization Code window appears.

15 Type the reference number and authorization code (obtained remotely from the administrator—the administrator receives this information after entering a new user into the PKI).

16 Click **Next**.

The Entrust Certificate PKI Accessibility window appears.

17 Click the appropriate button to indicate the location of the Entrust Certificate PKI.

OR

Click **I Don’t Know**, if that is the case.

18 Click **Next**.

When the PKI server is on the Internet or behind the firewall, the server is directly accessible. When the PKI server is behind the VPN Router, it is not directly accessible. The test option (I Don’t Know where the PKI server is) attempts to establish a TCP connection to ports 389 and 709 to the PKI listed in the entrust.ini file. The client tries for 30 seconds before it times out. If the connection times out or is refused, the wizard assumes that the PKI is not directly accessible.

19 Select a dial-up connection from the **Dial-Up Networking Profiles** list if you need a dial-up connection to access the Internet.

20 Review the information in the **Generate Certificate** window.

This window shows the information that generates the authentication certificate and appears only if the PKI server is behind the firewall.

21 If the information is correct, click **Finish** to connect to the PKI, which generates a new certificate.

Obtaining a certificate when Entrust PKI server is behind the firewall and VPN Router

Obtain a certificate when the Entrust PKI server is behind the firewall and the VPN Router.

When the Entrust PKI Certificate server is behind the firewall and the VPN Router, you must also provide an LDAP user ID and password in the User Identification window. This information establishes a temporary tunnel used only to obtain a new certificate. After the server generates the certificate, the user no longer needs the temporary LDAP user ID and password because the server uses the new certificate.

You must obtain this information from the network administrator. The administrator creates a special group for this user name and password so that a filter permits access only to the PKI for this user.

1 Choose a directory in which to store the .epf file.

2 Name the **.**epf file.

3 Select a password.

4 Type the entrust reference number and authorization code (obtained from the network administrator).

5 Type the host name or IP address of the remote VPN Router.

6 Click **Next**.

The Dialup Connection window appears.

7 Determine whether to establish a dial-up connection to the Internet.

If you select **Yes**, select an option from the Dial-up Networking Profile list to establish a connection to the Internet.

OR

Click **Next**

The Generate Certificate window appears. The Generate Certificate window shows the key information that the PKI Entrust server uses for the temporary VPN connection, excluding the password.

8 Click **Finish**.

The Success window appears, or an error message indicates why the server did not generate a certificate.

Entrust roaming profiles support

A roaming certificate resides on an external server. After you enroll for a certificate, the certificate is on the roaming server rather than on the user PC or smartcard. You log on to Entrust Entelligence, authenticate to the roaming server, and receive the certificate, which you then use to authenticate Entrust-ready applications, such as VPN.

The Avaya VPN Client supports existing clients with .epf files on their local computer (with or without Entrust Entelligence) and also supports roaming users who use Entrust Entelligence.

Offline and online support for roaming profiles

The Avaya VPN Client provides an online or offline configuration that pertains to where the CA server is in relation to the client:

- Online means that the CA server is accessible to the client before you establish the tunnel.
- Offline means that you must establish the tunnel before the client PC can access the CA server.

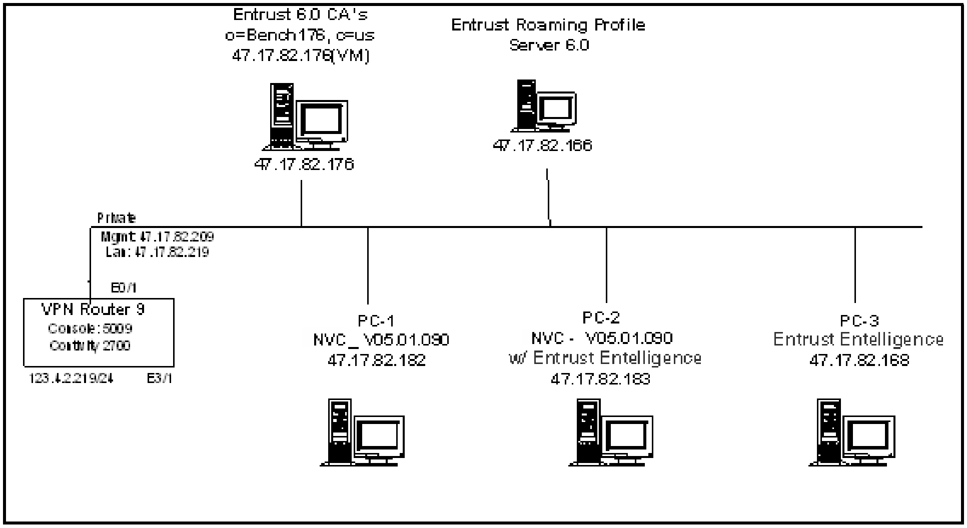
The client can use an online or offline roaming profile:

- Online roaming—the client logs on with the credentials that the roaming profile server supplies. The roaming profile server must be accessible to the client PC before tunnel establishment.
- Offline roaming—the client uses stored cache files for its credentials. The client uses offline roaming if the roaming server is unreachable.

The roaming server and LDAP must be accessible to the client. If you cannot access the servers, you must enable the firewall and open the appropriate ports to the clients.

The following figure shows PCs that connect to a roaming server.

Figure 2 PCs connected to roaming server



Configuring Entrust for roaming profiles

You configure the following three components for roaming profiles:

- CA server
- roaming profile server
- roaming profile clients

Configuring the CA server

Configure the CA server to use roaming profiles.

1. From the registration authority (RA), export, edit, and then import the **mastercert.spec** file.
2. Edit the **entmgr.ini** file.
3. Edit the **entrust.ini** file and place it into the C:\WINNT directory.
4. Add a **Roaming User**.

Editing the mastercert.spec file

Edit this file only if you require offline roaming.

The following example configures profile use for roaming users:

```
offline_prof_use=1.2.840.113533.7.77.20,BitString,<offline_prof_us
e>
```

The following must appear on one line, with no wrap or line feed:

```
offline_prof_use=Boolean,Offline Roaming allowed:,Allow use of
roaming profiles in offline mode.,Range,0,1
```

Editing the entmgr.ini file

Edit this file only if you require offline roaming:

```
[Default Variable Values]
offline_prof_use=1
```

Editing the entrust.ini file

Edit the entrust.ini file based on the roaming requirements. After you edit the file, place it on the CA Server, roaming profile server, and client PC that uses a roaming profile.

Use the following edits to enable roaming profiles online. Place each entry on a separate line.

```
ProfileServer=<IP or DNS of Profile Server>+640
ProfileServerDN=<FDN of Roaming Profile user you create on RA>
RoamingIDField=<User ID attributes>
RoamSearchBase=<Search base of your CA>
```

Use the following edits to enable roaming profiles offline (optional). Place each entry on a separate line.

```
DefaultProfileLocation=<Path to store the cached files>
OfflineProfileLifetime=<# of days the cached files will be valid>
```

Use the following edits to enable proxy mode (optional):

```
RoamGetFilesFromServer=<Enable(1) or Disable(0)) Proxy Mode>
```

➡ **Note:** Proxy mode requires additional overhead, so transactions take longer to authenticate than with the normal operational mode.

Adding a roaming profile administrator from RA

Add a roaming server in Entrust/RA to create its Entrust profile. If you plan to use multiple servers with a separate profile for each, create a profile for each instance of roaming server before you attempt to encrypt each one.

1 Log on to Entrust/RA.

The Entrust/RA window appears.

2 Choose **Users**, **New User**.

The New User dialog box appears.

3 On the **Naming** tab, select **Web Server** or **Person** from the **Type** list.

If you choose Web Server, you do not need to type a first and last name. You must type a first and last name if you select Person.

4 In the **Name** box, type a name for the server.

5 In the **Description** box, type a description of the server.

The Description box is optional. Use this box to record important information about a roaming server (for example, the IP address).

6 In the **Add to** list, select the searchbase under which to add the roaming server.

By default, CA Domain Searchbase appears first and is often the top level searchbase in an organization.

7 Select **Create Profile**.

8 Click **Certificate info property**.

9 Select **Enterprise** in the **Category** list.

10 Click **Profile Server (Profileserver Certificates)** in the **Type** list.

11 Click **OK**.

The Create Profile dialog box appears.

Creating a roaming profile administrator

Create a roaming profile administrator from RA.

1 If you do not select **Create Profile** in Step 7 of the preceding procedure, the **New User** dialog box closes and you return to Entrust/RA. To open the **Create Profile** dialog box from Entrust/RA, right-click **Roaming Server** in the right pane, and then click **Create Profile** from the menu.

2 At the top of the **Create Profile** dialog box, click **Create Desktop Profile**.

Do not click Create roaming profile, if it appears—you use this option to create roaming users.

3 In the **Name** box, type a name for the roaming profile.

4 In the **Location** box, specify a location for the roaming server profile or accept the default.

5 In the **Password** box, type a password.

6 In the **Confirm** box, type the password.

7 Click **OK**.

Depending on the company security policy, one or more Authorization Required dialog boxes appear. Authorize the transactions if required, and click **OK**.

A dialog box appears that displays the distinguished name of the roaming server you just added and the location of the .epf file.

Installing and configuring the roaming profile server

To install the roaming profile server, the required software is Entrust Authority Roaming Server 6.0.

1. Make sure you have the roaming administrators profile files and entrust.ini files. Save them on the hard drive. Save the entrust.ini to C:\WINNT.
2. Install the software. No license is required; if you select the configure utility, the software goes to the same location.

To configure the roaming profile server

1. On the **General** tab, enable **Automatic/Unattended startup**.
2. Type the password.
3. On the **Log** tab, enable **Send logs to file** and **Browse to a file**.
4. On the **LDAP** tab, enter configuration information for the Entrust Directory server.
5. Start the service. You can configure it to start up automatically after you restart the computer.

Configuring roaming profile clients

The following is the required software:

- Avaya VPN Client V05_11 or newer
- Entrust Entelligence 5.02 or newer

To configure roaming profile clients

1. Place the following three Entrust DLLs in the C:\WINNT directory:
   - kmpapi32.dll version 6.0.541.1210
   - enter.dll version 6.0.520.1241
   - etsesn32.dll version 6.0.531.1220
2. Place the edited entrust.ini in the C:\WINNT directory.

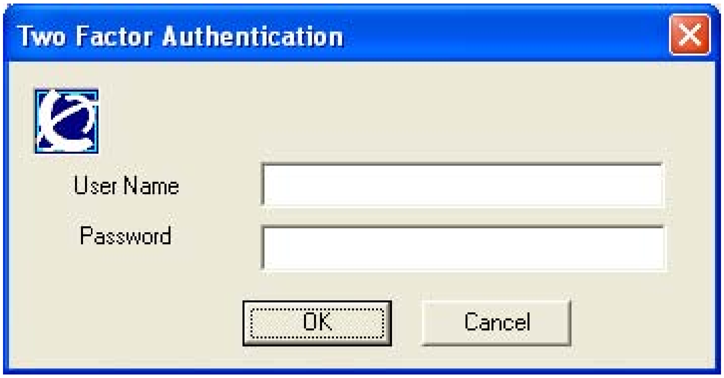
Entrust Entelligence and the client provide roaming profile support independently, or both can coexist on the same PC. You do not need to install Entrust Entelligence Client for the Avaya VPN Client to support roaming profiles.

Two factor authentication

Beginning with VPN Router 8.0 and Avaya VPN Client 8.01, you can use two factor authentication. If you enable two factor authentication on the router, the VPN user must supply two sets of credentials to log on to the router.

The user must first configure the client to use a digital certificate as described in "Configuring a certificate and smartcard connection" on page 21. After the client tries to connect to the router, the router uses the certificate for initial authentication. After the certificate authentication is complete, the router uses the secondary authentication credentials, a user name and password. A dialog box appears that prompts the user to provide the user name and password. You can store the user name and password locally or externally in a Remote Authentication Dial In User Service (RADIUS) or LDAP Proxy server. The following figure shows the dialog box that appears to the Avaya VPN Client user.

Figure 3 Secondary authentication dialog box



The user name and password that the user provides does not save for future sessions. Users must provide this information each time they establish a new session. For more information about how to configure two factor authentication on VPN Router, see *Avaya VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600).

Group security

You can use two types of group security as authentication methods:

- token
- group password

Token

This method is RADIUS authentication with a response only or challenge response token product such as RSA SecurID or PassGo.

Group password

Select this option for authentication to a RADIUS server. Use the group ID and password to authenticate against a defined user group on the VPN Router. The RADIUS server uses the user name and password to authenticate.

The Avaya VPN Client does not share the group password between local computer accounts. If you log on to the local computer by using a different user account than the one you use to create the Avaya VPN Client profile, you must reenter the group password. For example, you log on to the local computer as the administrator, create the client profile, and log off. If you then log on to the local computer with a different user account, you must reenter the group password in the client profile.

You must reenter the password regardless of how you install the Avaya VPN Client, as an application, as a service, or as a service with Avaya Graphical Identification and Authentication (NNGINA) mode. Reenter the password by choosing Options, Authentication Options, Group Security Authentication.

Windows domain logon

You can log on to the Windows domain in the following ways:

- Two-step domain logon (Windows service)
- Graphical Identification and Authentication (GINA)

Logging on with two-step domain

To log on to an existing Windows domain on the private side of the VPN Router, you must have a valid Windows domain account that is accessible from the private side of the VPN Router.

To log on to the Windows domain

1. Start the Avaya VPN Client.
2. Make a connection to the VPN Router that can access the Windows domain.
3. Log off from the current Windows user session.

   The Avaya VPN Service maintains the IPsec tunnel to the Windows domain.

4. Press **Ctrl+Alt+Delete** to log on to the Windows domain from the already established connection to the VPN Router.

GINA logon

A Graphical Identification and Authentication DLL provides an automated process to complete a Windows domain logon through a VPN tunnel. GINA implements the authentication policy of the interactive logon and performs all identification and authentication user interactions for the Windows system. You do not need to log on locally to launch the client, and then log off the local system to authenticate to the Windows domain.

The Avaya GINA (NNGINA), nngina.dll, launches and synchronizes a successful tunnel creation with the Avaya VPN Client and disconnects the VPN tunnel after you log off. After NNGINA makes a successful VPN connection, the Windows domain logon continues through the established VPN tunnel connection. GINA chaining detects the presence of a previously installed third-party GINA and passes all pass-through calls to that particular GINA.

Note: If you install GINA, Windows disables fast-user switching.

To enable the installed NNGINA, select Connect Before Logon on the Options menu.

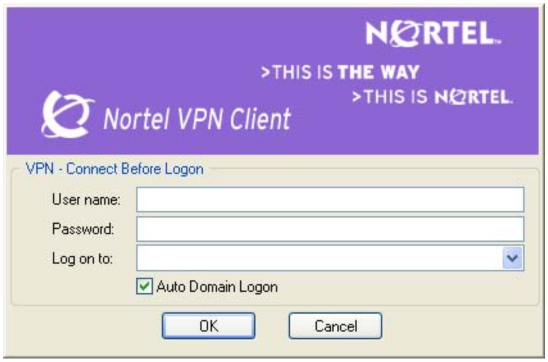
Logging in through the client connection

At system logon, use the following procedure to log on through an Avaya VPN Client connection.

Note: Auto domain logon is the default.

1 Press **Control+Alt+Delete**.

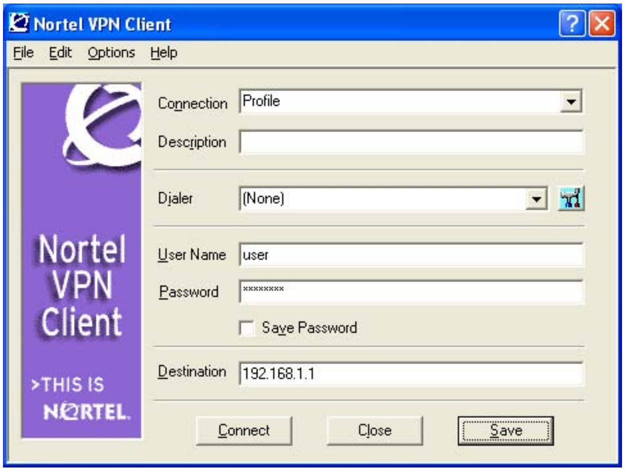
The NNGINA dialog box appears.



Note: If you do not want to use the Connect Before Logon feature after you enable it, click Cancel. The Windows domain logon window appears.

2 Type the Windows credentials, which you use to perform a local system logon.

The Avaya VPN Client appears.



Connection: Profile

Description:

Dialer: (None)

User Name: user

Password: ********

□ Save Password

Destination: 192.168.1.1

3 Type the VPN tunnel credentials.

The VPN tunnel connection is complete. The Windows domain logon automatically runs using the authentication credentials provided in the NNGINA dialog box. The Domain logon establishes by using the existing VPN tunnel connection.

Launching a tunnel prior to Windows authentication

To successfully launch Avaya VPN Client in previous versions of NNGINA, you must log on to the target domain at least once from the local system to create a cached user profile. The enhancement to NNGINA no longer requires a cached user profile, or for the user to log on to the target domain at least once before using NNGINA to log on. Also, because the tunnel establishes prior to Windows authentication, you can update Windows domain group policy during the course of a normal user log on.

Cached profile logon

To log on to the system using an existing local account to establish the VPN tunnel, you must select Cached Profile Logon from the Options menu. See “Options menu” on page 45. You need this NNGINA option when you use certificate authentication because the Avaya VPN Client must access the MS CAPI certificate store.

If the cached profile fails to load, the NNGINA and client continue trying to establish a tunnel prior to Windows authentication. As long as a user certificate is not required for tunnel authentication, this fallback option is successful.

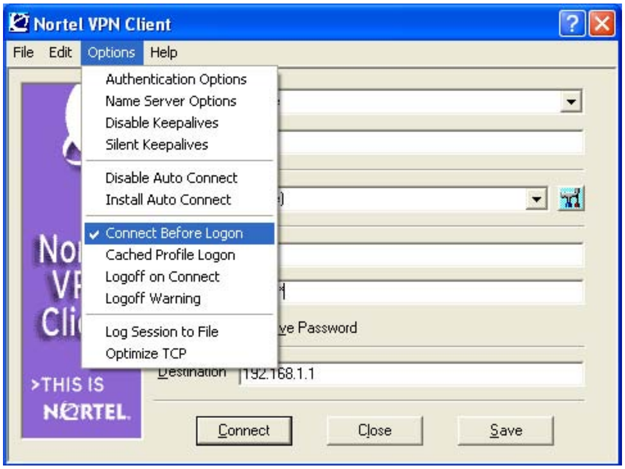
Note: The Windows domain administrator must configure the client workstation to allow access to the desired Windows domain.

You can either execute the current Avaya VPN Client Windows domain logon or use the client GINA by clearing Auto Domain Logon and logging on using an existing local user account. The Windows GINA window appears to complete the domain logon.

Enabling and disabling Connect Before Logon

To enable or disable Connect Before Logon, choose Options (see “Options menu” on page 45) and then select Connect Before Logon. The Avaya VPN Client GINA dialog box provides simultaneous Windows NT domain logon when you log on to the workstation. You must install the Avaya VPN Client with the GINA option.

Figure 4 Options menu



Destination 192.168.1.1

Uninstalling NNGINA/GINA chaining

You cannot uninstall NNGINA unless it is at the top of the GINA chain. If NNGINA is not at the top of the GINA list, uninstalling it breaks the GINA chain, and you receive notification from the software that indicates that you must uninstall third party GINAs before you can uninstall GINA. This can occur multiple times until NNGINA is at the top of the chain.

Incompatible third-party GINAs

Because some third-party GINAs conflict with NNGINA, a list of conflicting third-party GINAs is available to help you determine if the installation can proceed. The GinaList.ini file is in the custom installation directory. You can add additional conflicting third-party GINAs to the list.

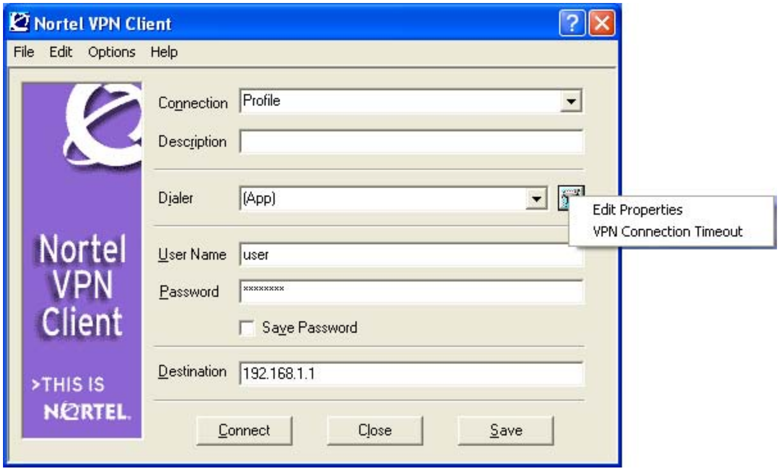
If the client detects an incompatible GINA during installation, it generates a comment in the line preceding the identified conflicting GINA.

For an example of the format of the GINA list. See “Format of GINA list” on page 71.

Application launch

To start the user-defined application before you start the client, select (App) from the Dialer list in the Avaya VPN Client logon window, see “Application launch window” on page 47.

Figure 5 Application launch window



Connection: Profile

Description:

Dialer: (App)

User Name: user

Password: ********

□ Save Password

Destination: 192.168.1.1

The application launch provides the following options:

- Edit Properties—configure detailed information about the application launch in the two boxes Executable filename include path and Friendly Name. The Friendly Name appears next to (App) after you complete the configuration.
- VPN Connection Timeout—configure the seconds of Avaya VPN Client connection timeout. The minimum value is 60 seconds, and no maximum value exists. The default value is 120 seconds.

Note: You must have Administrator privileges on the Windows workstation to make changes to the properties and timeout settings.

Optimizing the TCP window

If you optimize the TCP window, the client queries the TCP window size of the current physical adapter interface and also queries the TCP window size of the VPN adapter interface through the Windows registry. If these two values do not match, the client resets the TCP window size for the VPN adapter to match the TCP window size of the physical adapter. This action restarts the VPN driver to establish the new TCP window size on the VPN adapter interface. After the new TCP window size takes effect, you can establish a tunnel.

After you reset the TCP window configuration, the VPN adapter uses the Windows default TCP window size. This value is not always optimal for high latency connections such as wireless, cellular, and satellite networks.

To optimize the TCP window, choose Options, Optimize TCP. The default is disabled.

If you have administrator privileges, the following message appears: `VPN optimizing TCP`. If you do not have administrator privileges and you select Optimize TCP, the following message appears: `You need to reboot for Optimizing TCP to take effect`.

If the client runs in IPsec mobility mode and a difference exists in the TCP window sizes of the physical interface and the VPN interface, the change in window size does not take effect until the next restart of the client. This delay occurs because IPsec mobility must maintain tunnel connection during the interface change and restarting the VPN driver in this mode disconnects the tunnel.

Two registry keys exist for this feature. For more information about the registry keys and the flags defined for custom installation, see *Avaya VPN Router Installation and Upgrade — Client Software Release 8.01* (NN46110-409).

Banners

You can use one of the following banner types:

- Security banners
- TunnelGuard notify banners

Security banners

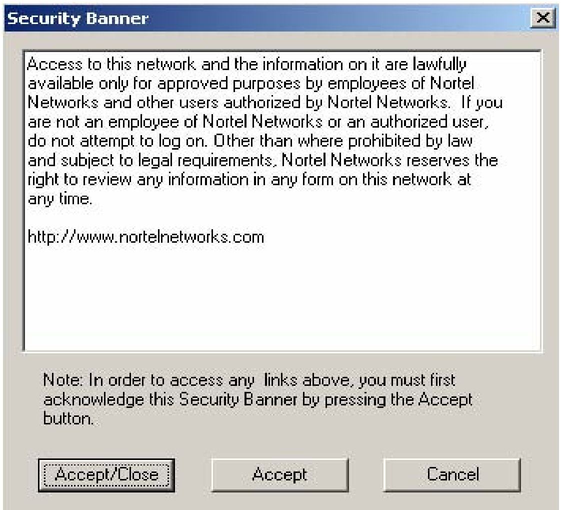
A security banner displays a message that is pushed from the server after a VPN tunnel establishes, if the banner is configured on the server. All traffic to the server is blocked until the user acknowledges the banner. The user has three options:

- Accept/Close—permits traffic to flow and the dialog box closes.

- Accept—permits traffic to flow, the security banner remains visible, and all links are available.
- Cancel—terminates the tunnel immediately.

The following figure shows the security banner dialog box.

Figure 6 Security banner



Security Banner

Access to this network and the information on it are lawfully available only for approved purposes by employees of Nortel Networks and other users authorized by Nortel Networks. If you are not an employee of Nortel Networks or an authorized user, do not attempt to log on. Other than where prohibited by law and subject to legal requirements, Nortel Networks reserves the right to review any information in any form on this network at any time.

http://www.nortelnetworks.com

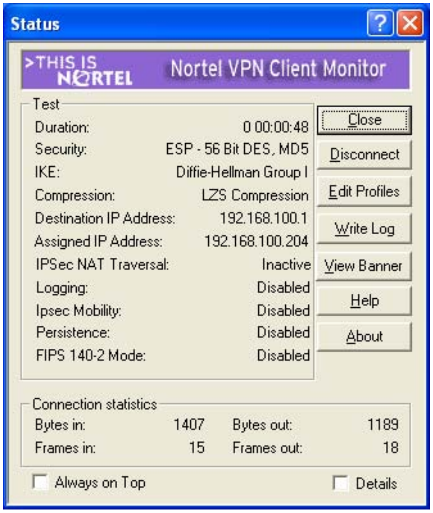
Note: In order to access any links above, you must first acknowledge this Security Banner by pressing the Accept button.

The security banner uses a timeout value. If the user does nothing for 2 minutes, the connection terminates.

A View Banner option exists on the status dialog box that the user can access to view the banner.

“View Banner option” on page 50 shows the dialog box with View Banner.

Figure 7 View Banner option



Test

Duration:	0 00:00:48
Security:	ESP - 56 Bit DES, MD5
IKE:	Diffie-Hellman Group I
Compression:	LZS Compression
Destination IP Address:	192.168.100.1
Assigned IP Address:	192.168.100.204
IPSec NAT Traversal:	Inactive
Logging:	Disabled
Ipsec Mobility:	Disabled
Persistence:	Disabled
FIPS 140-2 Mode:	Disabled

Connection statistics

Bytes in:	1407	Bytes out:	1189
Frames in:	15	Frames out:	18

□ Always on Top □ Details

Dynamic Domain Name System

If you enable dynamic Domain Name System (DNS) at the group level on the server, the DNS registration to the assigned DNS server occurs after you accept the security banner.

TunnelGuard Notify banner

If you enable TunnelGuard checking on the server, the server periodically checks for the existence of TunnelGuard Agent. If this check fails, the server sends a message to Avaya VPN Client. The contents of the message appear in a dialog box. For more information about this banner, see *Avaya VPN Router Configuration—TunnelGuard* (NN46110-307).

Tunneling modes

Three types of tunneling modes exist:

- mandatory
- split
- inverse split

Mandatory tunneling sends all traffic down the tunnel. Split tunneling specifies the tunnel networks, with all remaining traffic sent outside the tunnel. Inverse split tunneling specifies the nontunnel networks, with all remaining traffic sent inside the tunnel.

When Avaya VPN Client operates in split tunneling mode, it periodically checks the routing table on the client computer to determine if the table changes. The client performs this check for security reasons to detect intrusions and unauthorized access to the private network. After the client detects a routing table change, the tunnel disconnects.

For more configuration information about split tunneling, see *Avaya VPN Router Configuration—Basic Features* (NN46110-500).

IPsec mobility and persistence

IPsec mobility maintains IPsec connections for mobile users so that they can roam from subnet to subnet without terminating applications. IPsec mobility maintains a connection between the Avaya VPN Client and the VPN Router after the IP address changes. The Avaya VPN Client status monitor reports if roaming is enabled for the session.

When the client operates in IPsec mobility mode with split tunneling enabled, if the following changes occur, the client does not consider the routing table maliciously altered nor does it disconnect the tunnel:

- IP address change for an adapter
- adapter removed
- adapter plugged in and connected

For more information about IPsec mobility and persistence, see *Avaya VPN Router Configuration—Basic Features* (NN46110-500).

Coexisting with Microsoft IPsec Service

Avaya VPN Client can coexist with Microsoft IPsec Policy Service. Avaya VPN Client uses Network Address Translation (NAT) Traversal, User Datagram Protocol (UDP) wrapping to avoid conflicts if you enable or start the Microsoft IPsec Policy Service.

➡ **Note:** For Microsoft IPsec Policy Service to work, you must enable NAT Traversal for the group to which the user authenticates on the VPN Router.

For more information about how to configure the Avaya VPN Client to coexist with Microsoft IPsec Policy Service, see *Avaya VPN Router—Tunneling Protocols* (NN46110-503).

Chapter 2
Client control

This chapter describes how to control the Avaya VPN Client from a third-party application or script and includes the following topics:

- "DOS command line procedures" on page 53
- "Windows message handling" on page 58

DOS command line procedures

You can write an application to establish a tunnel with command-line switches. For example, you can collect a user name, password, and destination address in the application, and with that information launch the Avaya VPN Client (extranet.exe) to establish a tunnel.

To launch the Avaya VPN Client from the application, enter the following command:

```
ShellExecute() or CreateProcess()
```

To pass the user name and password, which the user supplies, to the application in the command line (the destination is the remote server), enter the following command:

```
Extranet.exe -u username,password,destination
```

If you use a Remote Authentication Dial In User Service (RADIUS) user name and password for authentication, enter the following commands:

```
Extranet.exe -r
username,password,destination,groupid,grouppassword
```

The following table lists the command line parameters that the Avaya VPN Client recognizes.

Table 2 Avaya VPN Client command line parameters

Switch	User entry	Description
/?	n/a	Opens a Help window for the command line parameters
-a	*<profile>*	Activates the connection profile to use
-o	*<profile>*	Opens the profile (makes the profile available for editing)
-d	*<profile>*	Indicates the connection profile to delete
-n	n/a	Creates a new connection profile using the Connection Wizard
-u	*<username,password,destination>*	Activates a connection with the supplied Lightweight Directory Access Protocol user information
-r	*<username,password,destination, groupid,grouppassword>*	Activates a connection with the supplied RADIUS user information
-e	*<Entrust.epf, password, destination>*	Activates the connection to the server
-t / -T	n/a	Shuts down the VPN tunnel connection and terminates the Avaya VPN Client application
-l / - log	n/a	Starts logging
-s / -S	-a, -e, -r, or -u	Runs in silent success mode, which hides the dialog boxes that appear during the connection
-fs/-FS	n/a	Modifies silent success behavior by suppressing error dialog boxes

Running in silent success mode

You can launch the Avaya VPN Client application with the -s or -S option to run in silent success mode. This mode hides the common dialog boxes that appear during the connection and provides less user interaction with the client. This mode suppresses all success dialog boxes; it does not suppress error dialog boxes.

Enter **`-s -a`** *`<profile>`* to use the connection profile.

Enter **-s -u <***username,password,destination***>** to activate a connection with the Lightweight Directory Access Protocol (LDAP) authentication.

Enter **-s -r** <*username,password,destination,groupid, grouppassword*> to activate a connection with RADIUS authentication.

Enter **-s-e** <*entrust.epf, password*> to activate a connection with Entrust authentication.

Enter **-sf/-FS** to suppress error dialog boxes.

Changing the group password

To overwrite the group password information, the Avaya VPN Client provides a set of command line options for the different authentication methods.

The syntax to overwrite the group password is

```
extranet.exe -auth <authentication type> -user <username>
-pwd <password> -gid <gid> -gpwd <group password> -serverip
<server ip> -pin <PIN> -code <tokenCode>
-profile <profile name>
altname <subj-alt-name> -alttype <number>
```

The authentication type can be one of the following:

```
0: User name, password login
1: Challenge response token card
2: SecureId hardware token
3: RADIUS and LDAP authentication
4: PassGo Defender
5: SecureId software token
6: Entrust certificate
9: MSCAPI certificate
10: use connection profile, other commandline inputs can overwrite
the profile content
```

For example, if -auth is 10, a profile decides the authentication type. The command line switch always overwrites the authentication type in profile.

Two additional command line switches are

- altname <subj-alt-name>
- alttype <number>

For the alttype command line switch, enter one of the following

```
1: CN_RFC822_NAME
2: CN_DNS_NAME
4: CN_DIRECTORY_NAME
6: CN_RESOURCE_LOCATOR
7: CN_IP_ADDRESS
8: CN_REGISTERED_ID
```

Some switches are optional if you use a profile as an authentication method. Switches that you provide overwrite the information in the profile and in the registry. You must use some switches, for example, password and group password; however, if you save the password or group password in the registry, those switches are optional.

Previous command line options do not cover all of the authentication methods (comma separated authentication information), but the command line options continue to work with the present release.

The following examples show the commands to use for the different authentication methods:

- If you use user name and password logon, enter the following commands:

  extranet.exe -auth 0 -user *<username>* **-pwd** *<password>* **-serverip** *<server ip>*

  extranet.exe -auth 10 -profile *<profilename>* **-user** *<username>* **-pwd** *<password>* **-serverip** *<server ip>*
- If you use the challenge response hardware token, including the PassGo token, enter the following commands:

  extranet.exe -auth 1 -user *<username>* **-serverip** *<serverip>* **-gid** *<gid>* **-gpwd** *<group password>*

  extranet.exe -auth 10 -profile *<profilename>* **-user** *<username>* **-serverip** *<serverip>* **-gid** *<gid>* **-gpwd** *<group password>*
- If you use the SecurID hardware token, enter the following commands:

```
extranet.exe -auth 2 -user <username> -pin <PIN> -code
<tokenCode> -serverip <server ip> -gid <group id> -gpwd
<group password>
```

```
extranet.exe -auth 10 -profile <profilename> -user
<username> -pin <PIN> -code <tokenCode> -serverip <server
ip> -gid <group id> -gpwd <group password>
```

- If you use a simple group ID and password, enter the following commands:

```
extranet.exe -auth 3 -user <username> -pwd <password>
-serverip <server ip> -gid <group id> -gpwd <group
password>
```

```
extranet.exe -auth 10 -profile <profilename> -user
<username> -pwd <password> -serverip <server ip> -gid
<group id> -gpwd <group password>
```

- If you use a PassGo software token, enter the following commands:

```
extranet.exe -auth 4 -axentPath <axentpath> -serverip
<server ip> -gid <group id> -gpwd <group password>
```

```
extranet.exe -auth 10 -profile <profilename> -axentPath
<axentpath> -serverip <server ip> -gid <group id> -gpwd
<group password>
```

- If you use a SecurID software token, enter the following commands:

```
extranet.exe -auth 5 -user <username> -pin <PIN>
-serverip <server ip> -gid <group id> -gpwd <group
password>
```

```
extranet.exe -auth 10 -profile <profilename> -user
<username> -pin <PIN> -serverip <server ip> -gid <group
id> -gpwd <group password>
```

- If you use Entrust, enter the following commands:

```
extranet.exe -auth 6 -user <entrust profile path> -pwd
<entrust profile password> -serverip <server ip>
```

```
extranet.exe -auth 10 -profile <profilename> -user
<entrust profile path> -pwd <entrust profile password>
-serverip <server ip>
```

```
extranet.exe -auth 6 -user <profilename> -pwd <entrust
profile password> -altname <subj-alt-name> -alttype
<number> -serverip <server ip>
```

- If you use Microsoft CryptoAPI (MS CAPI), enter the following commands:

```
extranet.exe -auth 9 -user <MACAPI certificate string>
-serverip <server ip>
```

```
extranet.exe -auth 10 -profile <profilename> -user
<MACAPI certificate string> -serverip <server ip>
```

Windows message handling

If the application supplies a Windows message and Windows handle for the application, the Avaya VPN Client notifies the application after the connection establishes. The following table shows the command line parameters for Windows message handling.

Table 3 Windows message handling command line parameters

Switch	User entry	Description
-h	*<Windows handle>*	The Windows handle of the application that launches the Avaya VPN Client
-m	*<message handle>*	The Windows message to post to the handle, passed in -h, after the connection establishes or fails to establish

A sample command line string to launch the Avaya VPN Client and post a message back to the launching application is

```
Extranet.exe -h 1234 -m 1225 -a MyExtraNetConnection
```

Following the preceding example, after the tunnel either connects or fails to connect, the IPsec client responds with the following:

```
PostMessage(1234, 1225, (IPsec Hwnd), True/False).
```

After the message posts back to the Windows handle of the application, lParam indicates success or failure.

After the tunnel establishes, lParam is True; after tunnel establishment fails, lParam is False. The server does not report additional error handling because the IPsec client informs the user about why the connection fails.

To disconnect the extranet connection, post a WM_USER Message (PostMessage) to the Windows handle of the IPsec client (enter FindWindow for the title of the Avaya VPN Client window). Configure lParam to True to disconnect the tunnel. If you configure lParam to False and issue a SendMessage instead of a PostMessage, the IPsec client informs the user if it connects (True) or not (False).

Note: To successfully terminate the client by command line with a relative path argument, as DOS requires, you must include the Avaya VPN Client path in the DOS PATH environment variable. Alternatively, you can pass the absolute path to the client by command line if the path is within quotation marks. For example, from Windows Start, Run, Open, c:\program files\avaya\extranet.exe -t fails unless you enclose the path to the client in the PATH environment variable. However, “C:\Program Files\Avaya\Extranet.exe” -t successfully terminates the Avaya VPN Client application.

Appendix A

This Appendix includes the following topics:

- “File, icon, and bitmap customization” on page 61
- “Format of GINA list” on page 71
- “Microsoft Windows Installer command line options” on page 72

File, icon, and bitmap customization

When you use the custom installation kit, you replace files in the directories under the Client\Domestic\CDROM section of the installation disk. You can also change some properties in the Microsoft Windows Installer (MSI) file. The following list details how to make those changes:

- To customize the profiles.dat file, replace the profiles.dat file in the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client directory.
- To customize the readme.txt file, replace the readme.txt file in the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client directory.
- To customize the Entrust file, do the following:
  - — Replace the entrust.ini file with your own entrust.ini config file in the \Client\Domestic\CDROM\Windows directory.
  - — Configure NN_ENTRUST property to 1.
- To customize icons, do the following:
  - — Configure property NN_CUSTOMICON=1.
  - — Replace the icon files and bitmap files in the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory.
- To customize the Product name, modify the Property Table: change ProductName=<customized name>.

- To customize the default installation path, update the Directory Table: INSTALLDIR and all parent folders, if necessary.
- To customize the default as InstallAsService and InstallGina, do the following:
  - — InstallAsService: Modify Property Table, change INSTALLLEVEL=200.
  - — InstallGina: Modify Property Table, change INSTALLLEVEL=300.

File customization

The two files you can customize are

- “Profiles.dat” on page 62
- “Group.ini” on page 65

Profiles.dat

To preconfigure the Avaya VPN Client with profiles, including information such as the authentication type and destination, you must distribute a profiles.dat file that contains the custom installation files. If you use the Avaya VPN Client to create user profiles, the client automatically creates a profiles.dat file in the installation directory, and you can distribute it to the users. Before you add the file to the custom installation, edit the file to remove the user name reference so that users can type their own user name.

Note: You must save a new profiles.dat file in text document format. If you save the file in rich text format (RTF) or in Word document format, the Avaya VPN Client does not recognize some of the formatting, and as a result, does not define the users.

If the file resides in the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client directory, the installation procedure copies the file to the appropriate directory and overwrites the existing profiles.dat file.

Define each connection profile between square brackets ([ ]), for example, [MyVPNConnection].

The following entries represent the profiles.dat file that resides in each Profile section:

- Description—user interface description field
- Dialup—dial-up profile

  The value None indicates that a dial-up profile does not exist.
- Username—user interface user name, or the .epf file of the user when you use Entrust authentication
- TokenType—used in combination with UseTokens to indicate the type of authentication

The following table shows the combined settings that the client supports.

Table 4 Supported UseTokens and TokenType settings

UseTokens	TokenType
0	0. Username and password authentication type
1	1. Challenge response hardware token (includes PassGo hardware token)
1	2. SecureID hardware token
0	3. Remote Authentication Dial In User Service and Lightweight Directory Access Protocol authentication
1	4. PassGo software token
1	5. SecureID software token
0	6. Entrust certificate
0	7. (Reserved)
0	8. (Reserved)
0	9. Microsoft CAPI stored certificate
0	10. Connection profile

- UsePAPGroup—0 indicates no Remote Authentication Dial In User Service (RADIUS) authentication; 1 indicates RADIUS authentication.
- GroupName—Options, Authentication Options dialog box, Group Name box.
- SavePassword—0 indicates that the user did not save the PIN or password; 1 indicates that the user did save the PIN or password.

- Server—IP address or host name of the server with which to establish a connection.

Sample profiles.dat file

```
[VPN Your City]
Description=Company Name
Dialup=(None)
Username=smith
UseTokens=0
TokenType=3
GroupName=VPN Router_VPN
SavePassword=0
Server=130.130.130.13
```

Profiles.dat example

The following is an example of a profiles.dat file:

```
[Profile Name]
Description=
Dialup=(None)
Username=name
UseTokens=0
TokenType=0
UsePAPGroup=0
GroupName=
SavePassword=0
Server=
primaryDNS=
secondaryDNS=
primaryWINS=
secondaryWINS=
domainName=
DisableKeepalive=0
EnableSilentKeepalive=0
```

Group.ini

The installation configures the registry with temporary text group passwords. The first time you run the client after installation, the client encrypts and deletes text group passwords. When the client distributes group passwords this way, users never need to enter the information. Instead, users can rely on their token cards and PINs, or RADIUS passwords for connection protection. You cannot preconfigure PINs or user-level passwords, only group-level passwords. The following table shows the settings for the group.ini file.

Table 5 Settings for group.ini file

Field	Description
[ProfileNames]	The name of the section that the installation looks for to send the names that you configure within this file. You must use this field as the heading.
1=MyExtranetConnection	Profile name that exists in profiles.dat.
2=OtherExtranetConnection	Profile name that exists in profiles.dat.
3=AnotherExtranetConnection	Profile name that exists in profiles.dat.
GroupPW=mygrouppassword	The text group password taken from the router under Profiles, Groups, Edit: IPsec Configure settings.
NoSavePassword=1	Prevents the user from trying to save the user password or PIN; you can configure this password on Profiles, Groups, Edit: IPsec Configure settings.
[MyExtranetConnection]	Profile name of the connection.

Sample group.ini:

```
[VPN City1]
GroupPW=password
NoSavePassword=1
[VPN City2]
GroupPW=password2
NoSavePassword=2
```

Note: The corresponding profile entry must contain an authtype that uses group authentication. If the entry does not contain this authtype, the client does not look for the group ID and group password when it displays the authentication options.

The group.ini file is at the same directory level as the Avaya VPN Client .msi file. The default name for this file is group.ini. You can change the name of the file using NN_GROUP_INI_FILE.

Icon customization

You use the custom client icon facility to insert your corporate icons in place of the existing icons for the client. Four Avaya icon groups exist that you can replicate, and within each of the four, you can create different indicators for activities, such as sending or receiving data or establishing a connection.

The customizable installation files are in the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory on the Avaya CD. Select all of the files and paste them into an empty directory on the PC called, for example, Custom Install.

Perform the following three steps to use a custom icon:

1. Create the icon.
2. Rename the icon according to the Avaya custom icon conventions.
3. Copy the renamed icon to the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory.

You must follow these steps for each of the following icon groups:

- Avaya VPN Client application icon
- Avaya VPN Client task bar icons
- Avaya VPN Client connecting icons

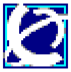
Two to four different representations of the group icon exist within each group. You can create icon bitmaps in whatever style you prefer; however, the Avaya icons convey a message for the action, such as data transfer activity or establishing a connection.

The following sections describe the icon types that you can create, and show where the icon appears in the client application.

Client application icon (eacapp.ico)

Use the client application icon eacapp.ico (see "Client application icon" on page 67) in place of the corporate icon, in the top-left corner of the main application window, while the client establishes the connection and during disconnection.

Figure 8 Client application icon



This icon is also the desktop shortcut icon when you create an autoconnect shortcut from the Create Shortcut selection under the client File menu. The icon appears in the following program folder that is created during the installation process:

Start, Program Files, Avaya, VPN Client

To replace the client application icon:

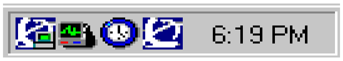
1. Create an icon called **eacapp.ico**.
2. Copy the icon to the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory.

Client task bar icons

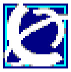
Task bar icons appear in the task bar to indicate data activity through the tunnel.

To replace task bar icons, do the following:

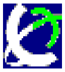
1. Create the following four icons:
   - **blinknone.ico**
   - **blinkright.ico**
   - **blinkleft.ico**
   - **blinkboth.ico**
2. Copy the icons to the target path in the CD ROM kit. The following figure is a sample with four icons created.



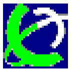
The following figure (Blink none [blinknone.ico]) shows a task bar icon that indicates that the client is running, but not currently transferring data.



The following figure (Blink right [blinkright.ico]) shows a task bar icon that indicates that the client is transmitting data through the tunnel.



The following figure (Blink left [blinkleft.ico]) shows a task bar icon that indicates that the client is receiving data into the tunnel.



The following figure (Both [blinkboth.ico]) shows a task bar icon that indicates that the client is both transmitting and receiving data through the tunnel.

The following figure (Client connecting icons) shows an icon group that shows activity during the client connection process. The group shows activity through a cycle of four different icons with an arrow pointing clockwise through each of the four quadrants of the circular icon.

To replace the client connection icons, do the following:

1. Create a series of icons and rename them with the following names:
   - connect1.ico
   - connect2.ico
   - connect3.ico
   - connect4.ico
2. Copy the icons to the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory.

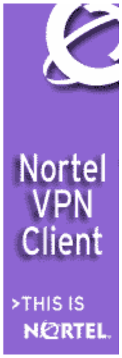
Bitmap customization

This section describes how to insert custom bitmaps in the main client dialog box message, the client status message, and the Extranet Connection Manager dialog box.

Client dialog bitmap (eacdlg.bmp)

The following figure shows the bitmap on the main dialog box of the client.

Figure 9 VPN Client bitmap



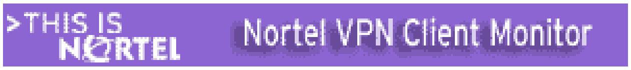
To replace the main dialog bitmap with a custom bitmap, do the following:

1. Create a 16-color bitmap that is 93 x 279 pixels.
2. Name the bitmap **eacdlg.bmp**.
3. Copy the bitmap to the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory.

Client status bitmap (eacstats.bmp)

The following figure shows the bitmap on the status dialog box of the client. This bitmap is visible only after you establish a tunnel.

Figure 10 Client status bitmap



To replace the status bitmap with a custom bitmap, do the following:

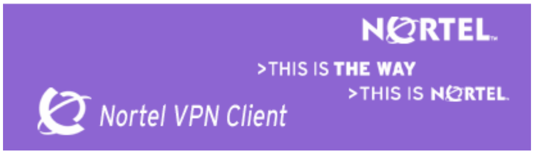
1. Create a 16-color bitmap that is 303 x 32 pixels.
2. Name the bitmap **eacstats.bmp**.
3. Copy the bitmap to the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory.

You can copy all of the files from the \Client\Domestic\CDROM\program files\Avaya\Avaya VPN Client\Icons directory onto diskettes, or you can put them into a network directory for corporate clients to retrieve.

Client GINA bitmap (nnginadlg.bmp)

You can brand or customize the Avaya VPN Client Avaya graphical identification and authentication (NNGINA) dialog box. You can also customize and replace the bitmap that appears on the graphical identification and authentication (GINA) dialog box; see the following figure.

Figure 11 GINA bitmap



The client checks for a new customized bitmap each time the dialog box initializes. The NNGINA looks for a custom bitmap named nnginadlg.bmp in the installation directory under the icons folder. If you install the Avaya VPN Client in the D:\Program Files\Avaya directory, the NNGINA looks for the custom bitmap as D:\Program Files\Avaya\icons\ nnginadlg.bmp. The Avaya VPN Client NNGINA bitmap is 417 X 113; the client scales custom bitmaps of a different size to fit the dialog box.

You must install the Avaya VPN Client as a service, and the NNGINA verifies this configuration.

Format of GINA list

The format of the GinaList.ini is

```
#Following Ginas conflict with Avaya NNGINA.

#The comment line right above the Gina DLL will be shown to users if
it's detected.

#Cisco Gina DLL

CSGina.dll

#X Gina DLL

X.dll
```

Microsoft Windows Installer command line options

You require Windows ® Installer V 3.01.4000.1823.

Enter the following command to use Microsoft Windows Installer command line options:

```
msiexec /Option <Required Parameter> [Optional Parameter]
```

Use the options in the following table to control the level of user interaction when you install the client.

Table 6 Windows Installer command line options

Options	Parameters	Meaning
Install options	</package | /i> <Product.msi>	Installs or configures a product
	/a <Product.msi>	Administrative install—installs a product on the network
	/j<u|m> <Product.msi> [/t <Transform List>] [/g <Language ID>]	Advertises a product—m to all users, u to current user
	</uninstall | /x> <Product.msi | ProductCode>	Uninstalls the product
Display Options	/quiet	Quiet mode, no user interaction
	/passive	Unattended mode—progress bar only
	/q[n|b|r|f]	Sets user interface level: n—No UI b—Basic UI r—Reduced UI f—Full UI (default)
	/help	Help information
Restart Options	/norestart	Do not restart after the installation is complete
	/promptrestart	Prompts the user for restart if necessary
	/forcerestart	Always restart the computer after installation

Table 6 Windows Installer command line options (continued)

Options	**Parameters**	**Meaning**
Logging Options	/l[i|w|e|a|r|u|c|m|o|p|v|x|+|!|*] <LogFile>	i—Status messages w—Nonfatal warnings e—All error messages a—Start up of actions r—Action-specific records u—User requests c—Initial UI parameters m—Out-of-memory or fatal exit information o—Out-of-disk-space messages p—Terminal properties v—Verbose output x—Extra debugging information + —Append to existing log file ! —Flush each line to the log * —Log all information, except for v and x options
	/log <LogFile>	Equivalent of /l* <LogFile>
Update Options	/update <Update1.msp>[;Update2.msp]	Applies updates
	/uninstall <PatchCodeGuid>[;Update2.msp] / package <Product.msi | ProductCode>	Removes updates for a product

Table 6 Windows Installer command line options (continued)

Options	Parameters	Meaning
Repair Options	/f[p|e|c|m|s|o|d|a|u|v] <Product.msi | ProductCode>	Repairs a product p—only if file is missing o—if file is missing or an older version is installed (default) e—if file is missing or an equal or older version is installed d—if file is missing or a different version is installed c—if file is missing or checksum does not match the calculated value a—forces the reinstallation of all files u—all required user-specific registry entries (default) m—all required computer-specific registry entries (default) s—all existing shortcuts (default) v—runs from source and recaches local package
Setting Public Properties	[PROPERTY=PropertyValue]	

For more information about the command line syntax, see Microsoft Windows Installer Software Development Kit (SDK).

When you run the /uninstall or /x command, you must provide either the MSI file or the MSI ProductCode. If the MSI file is not available or not easily found, you must determine the ProductCode. The ProductCode is in the Windows registry for the Avaya VPN Client entry at:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

The UninstallString key provides the complete command line including the ProductCode for uninstall.

You can also use tools such as MSI Inventory (msiinv.exe) or Windows application program interface (API) calls to determine the ProductCode. For more information, see the Windows Installer SDK.

Index