Administrator Guide
Avaya VPN Gateway

9.0
NN46120-105, 04.02
August 2012

Notice

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 Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya 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 materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the 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://www.avaya.com/support/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 other 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

Chapter 1: Preface

The *Avaya VPN Gateway Administrator Guide* contains example configurations and instructions on how to administer your Virtual Private Network (VPN).

Who Should Use this Book

This guide is intended for VPN administrators. As a VPN administrator, you are responsible for managing certain configuration parameters of a virtual private network that is hosted by an Internet Service Provider (ISP). The ISP has set up the basics of your VPN using the AvayaVPN Gateway (AVG) software. This guide assumes that you are familiar with Ethernet concepts and IP addressing. All IP addresses are examples and should not be used as-is.

Related documentation

For full documentation on installing and using the many features available in the VPN Gateway software, see the following manuals:

- *Avaya VPN Gateway Command Reference* (NN46120-103). Describes each command in detail. The commands are listed for each menu, according to the order they appear in the Command Line Interface (CLI).
- *Avaya VPN Gateway Application Guide for SSL Acceleration* (NN46120-100). Provides examples on how to configure Secure Socket Layer (SSL) Acceleration through the CLI.
- *Avaya VPN Gateway CLI Application Guide* (NN46120-101). Provides examples on how to configure VPN deployment through the CLI.
- *Avaya VPN Gateway BBI Application Guide* (NN46120-102). Provides examples on how to configure VPN deployment through the Browser-Based Interface (BBI).
- *Avaya VPN Gateway User Guide* (NN46120-104). Describes the initial setup procedure, upgrades, operator user management, certificate management, troubleshooting and other general operations that apply to both SSL Acceleration and VPN.
- *Avaya VPN Gateway Administrator Guide* (NN46120-105). VPN management guide intended for end-customers in a Secure Service Partitioning configuration.
- *Avaya VPN Gateway Configuration - Secure Portable Office Client* (NN46120-301). Gives the feature list and provides general information about Secure Portable Office (SPO) based VPN client.

- *Avaya VPN Gateway VMware Getting Started Guide* (NN46120–302). Describes how to install, configure, and deploy the Avaya VPN Gateway VMware appliances.
- *Avaya VPN Gateway Release Notes* (NN46120-400). Lists new features available in version and provides up-to-date product information.
- *Avaya VPN Gateway Troubleshooting Guide* (NN46120-700). Describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway (AVG).

The preceding manuals are available for download (see Customer service on page 10.

Customer service

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

Navigation

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at http://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 documentation

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

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 http://www.avaya.com/support.

Chapter 2: New in this release

The following sections detail what's new in *Avaya VPN Gateway Administrator Guide (NN46120-105)* Release 9.0.

Features

The following new features have been added to this release.

IPsec Two Factor authentication for Avaya VPN Gateway

Release 9.0 adds a two factor authentication method for authentication between servers and clients. When assigning authentication servers, you have the option to specify a second authentication server to use after the first one succeeds.

IPsec Two Factor authentication adds more robust security by using client certificate authentication as first factor to represent "what user-has" and using other authentication methods as second factor, "what user-knows".

Configuring a new certificate authentication server automatically supports IPsec Two Factor authentication. IPsec Two Factor authentication supports only certificate authentication as primary servers and local, RADIUS or LDAP as secondary servers.

Refer to Secondary and Two Factor authentication on page 76 for more information on IPsec Two Factor authentication.

Android L2TP/IPsec support

Avaya VPN Gateway Release 9.0 adds support for clients connecting via L2TP/IPsec from Android devices. Android versions 2.x, 3.x, and 4.x are supported and an additional license key is not required.

For supported Android versions, refer to the compatibility matrix, *AVG 9.0 Release Notes* (NN46120–400).

AES 256 support for IPsec

Release 9.0.0 adds AES 256 support for IPsec.

Java RDP upgrade support

Release 9.0 upgrades JavaRDP client for better support of the latest Windows Terminal server. A new optional field was added for WTS links, KeyMap URL, a URL path that points to a custom key code definition file.

Net Direct Mac OS X support

Release 9.0 supports Net Direct Mac OS X 10.7 (Lion).

Secure Portable Office (SPO) support

Release 9.0 adds Ceedo support on all Windows 64 bit platforms in virtualized mode.

Beginning with Release 9.0, you can download one of the two versions of SPO:

- Avaya Basic– contains basic software with Avaya 2050 IP Softphone and JRE 7.
- Avaya Contact Center (ACC)– contains all the applications and software of Avaya Basic with the addition of Avaya Contact Center Express Desktop 5.0 and Avaya One-X Client.

Both SPO version (Basic and ACC) use security restrictions on Ceedo environment. Next host resources are blocked inside Ceedo:

- Access to network shares and drives
- Access to printing
- Drag and drop
- Clipboard access

For more information on the Release 9.0 support, refer to *Configuration — Secure Portable Office Client Avaya VPN Gateway* (NN46120-301).

For more information about Secure Portal Office Client, see Appendix Secure Portable Office Client on page 327.

Other changes

The following are changes that are not feature-related:

- Please note, while the Avaya Endpoint Access Control Agent (formerly Tunnel Guard) can be configured through both the BBI and CLI, the CLI configuration is performed under the former Tunnel Guard context.

Chapter 3: The Browser-Based Management Interface

This chapter provides a general introduction on Browser-Based Management Interface (BBI), for example global commands, general site navigation, and on-line help.

VPN Administrator Account

For you to be able to access the BBI and administer your VPN, your Internet Service Provider (ISP) should have created a VPN Administrator's user account. Your ISP should also have provided you with the IP address and host name required to access your VPN Portal.

Starting the BBI

Follow these steps to launch the BBI:

1. Start your Web browser and connect to your VPN Portal.

   The Portal login page appears.

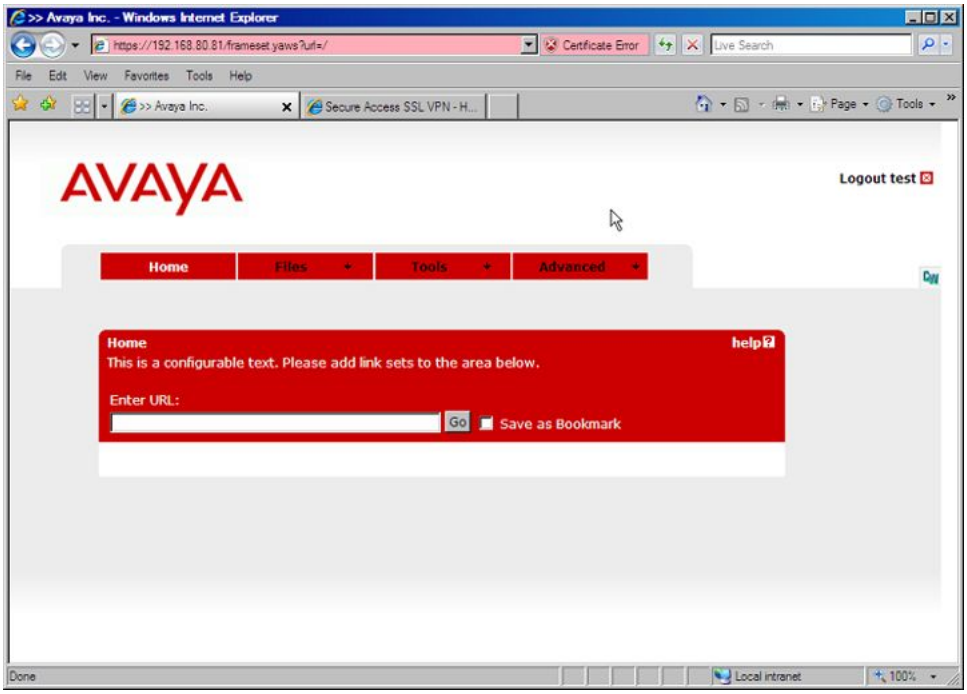
2. To log in, enter your user name and password in the **Username** and **Password** fields, respectively.

   Your credentials will be checked against a previously configured user record in the AVG's local authentication database or in an external authentication database.

3. The **Login Service** list box (if displayed), may contain different options for authentication services. If this is the case, your ISP should have informed you about which option to select.

4. Click **Login**.

   The Portal web page appears.



5. On the **Tools** menu, select **VPN Administration**.

   The BBI's first screen appears.

   The GUI lock warning message displayed at the top of the screen is only displayed just after accessing the BBI. If you switch to another BBI screen without unlocking the GUI, the message disappears.

   On the **GUI Lock** page (click the **Go to GUI Lock Page** button), you can lock the current BBI session by clicking the **Take The Lock** button. This step makes the BBI session owned by you and nobody else can make changes to the SSL VPN configuration through the BBI. To provide a message to other administrators logging in to the BBI while it is locked by you, enter a message in the **User Message** field.

   The padlock symbol in the BBI header does not indicate whether or not a VPN lock is taken. This is instead indicated with the color of the VPN Number text.

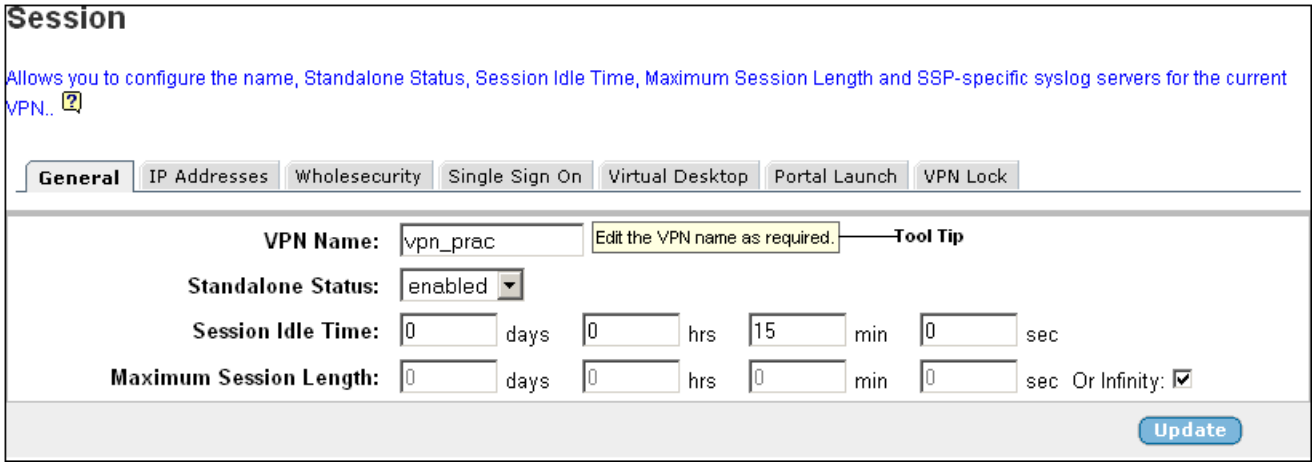
   - Brown color of the bread crumb indicates that no VPN lock has been taken
   - Green color of the bread crumb indicates that you currently have the lock.
   - Red color of the bread crumb indicates that another administrator has the lock.

   To release the lock, click the **Release The Lock** button.

   If necessary, a user having administrator rights can take over the lock from the administrator who currently has the lock. This is done in the same way as taking the lock the first time. Once the lock is taken over, the administrator will not be able to do any changes to the VPN. If the administrator has to do any changes then the lock needs to be taken over again.

Tool Tip

When a user points the cursor to a field in a screen, the information about that field is displayed in the text tool tip. In the following figure, information about the VPN name field is displayed in the tool tip.



Basics of the Browser-Based Interface

Interface Components

System Tree View

The System Tree View consists of items (VPN Gateways, Administration, and so on) representing the main categories for viewing information and configuring the system. By expanding an item, new items for the category's available forms will be displayed. You can expand several items at the same time, which gives you a good overview when configuring the system.

Note that some of the +-marked items display information when selected, besides showing sub-items.

Forms Area

The Forms Area contains fields that display information or allow you to specify information for configuring the system.

Global Link commands

These links are available from any page. The links display forms used for saving, examining, or aborting configuration changes.

Basic Operation

The Browser-Based Management Interface allows you to administer your VPN in the following manner:

- Select from a series of pages and sub-pages, and modify fields to create the desired configuration.
- When finished making changes on any given page, submit the form using the appropriate **Update** buttons. If you select a new form or end the session without submitting the information, the changes are lost.

  Most submitted changes are considered pending and are not immediately put into effect or permanently saved. Only a few types of changes take effect as soon as the form is submitted, for example changes to users and passwords.
- Use the global **Apply** form to save changes and make them take effect. The apply form allows the administrator to make an entire series of updates on multiple forms and then put them into effect all at once.
- Use the global **Diff** form to view pending changes before they are applied.
- Use the global **Revert** form to clear all pending changes; then continue the configuration session, or use the global Logout form to exit from the system. Logging out manually is preferred, though closing your browser manually or through inactivity (browser sessions automatically close after five minutes of inactivity) will also discard pending changes.

Note:

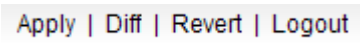
When multiple BBI administrator sessions are open at the same time, only pending changes made during your current session will be affected by the Diff, Revert, or Logout commands. However, if multiple BBI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

If the BBI is locked, no changes can be made by another operator using the BBI.

Global Command Forms

The global command links are always available at the top of each form:

These links summon pages which are used for logging out, saving, examining, or aborting configuration changes. Each global command page provides options to verify or cancel the command as appropriate.



Apply

The global Apply form is used for checking the validity of the current session's pending configuration changes, for saving the configurations change and putting them into effect.

The Global Apply form includes the following items:

- **Apply Changes** button. Applies pending changes.
- **Back** button. This button returns the previously viewed form.

Note:

The global Revert command clears pending changes. It cannot be used to restore the old configuration after the Apply Changes command has been issued.

Diff

The global Diff form provides a list of the current session's pending configuration changes.

The list displays a change record for each submitted update. Each record may consist of many modifications, depending upon the complexity of the form and changes submitted. Modifications are color coded:

- Green: New items that will be added to the configuration when the global Apply command is given and verified.
- Blue: Existing items that will be modified.
- Red: Configuration items that will be deleted.

The Diff list is cleared when configuration changes are applied or reverted, or when the administrator logs out or closes the browser window.

This command does not include pending changes made in other open CLI or BBI sessions.

Revert

The global Revert form is used for canceling pending configuration changes.

This form includes the following items:

- **Revert** button. This button cancels the current session's pending configuration changes. Applied changes are not affected. Pending changes made in other open CLI or BBI sessions are not affected.
- **Back** button. This button returns the previously viewed form without canceling pending changes.

Logout

The global Logout form is used to terminate the current user session.

This form includes the following items:

- Logout button. This button terminates the current user session. Any configuration changes made during this session that have not yet been applied will be lost. This command has no effect on pending changes in other open CLI or BBI sessions.
- Back button. This button returns the previously viewed form without logging out.

Note:

For thorough security, close all BBI windows (including help) after logging out.

Help

The Help form provides assistance with forms in the BBI. This is available in every page.

When you click the **Help** button, a new window appears with information appropriate to your current option:

The help window consists of the following areas:

- Pages— each page available in the Help Tree View contains a description of the corresponding form in the System Tree View. To load the actual form directly from the Help page, click the **LOAD** button located far right on the Help page's heading bar.
- Close (top right corner)—closes the Help window.

Site Map

The following Site Map table provides the list of sub-page menus and status/command labels for each form to aid navigation through the BBI.

Operational tab	Option	Menu	Submenu	Page
Config				
	VPN Gateways			
				General
				Traffic Trace
				IP Pool
				IP Sec
				Portal
				Link Sets
				Authorization
				Groups
				Authentication
				TunnelGuard
				VPN Client
				Advanced
Monitor				
	Dashboard			
	Monitor			
		Users		
		License Usage		
		IPsec Users		
		Idle Users		
		BO Tunnel Sessions		
		IP Pool Allocations		
		GUI Lock		

Operational tab	Option	Menu	Submenu	Page
		CLI Logins		
		About		
		Certificate		
	Statistics			
		Authentication		
		IPsec		
			Histograms	
			Statistics	
	Diagnostics			
		Trace		

Chapter 4: VPN Introduction

This chapter introduces the VPN (Virtual Private Network) subsystem.

VPNs allow remote users – for example mobile workers, telecommuters or partners – to access protected intranet or extranet resources such as applications, mail, files or web pages. The data are sent through a secure connection, either SSL (Secure Sockets Layer) or IPsec (Internet Protocol security).

What resources are accessible to the user is determined by the access rules configured for the group where the user is a member.

Access the intranet's resources in clientless mode, transparent mode, and/or Secure Portable Office (SPO) client mode:

- *Clientless mode*. From any computer connected to the Internet. The remote user connects to the VPN Portal through a secure SSL connection through the web browser. Once authenticated, the user can access intranet resources through the Portal's tabs. Clientless mode also enables download of the Net Direct client, a simple and secure method for accessing intranet resources through the remote user's native applications (see Clientless Mode on page 23).
- *Transparent mode*. From a computer with the SSL VPN client or the Avaya VPN Client (formerly the Contivity VPN client) installed. The term "transparent" means that the remote user will experience network access as if actually sitting within the corporate intranet (see Transparent Mode on page 26).
- *Secure Portable Office Client (SPO) mode*. The SPO client provides VPN access from portable storage such as USB flash memory and CDROM.

  The SPO client provides enhanced mobility, portability, and security compared to traditional VPN access methods. You can deploy and manage the SPO Client from the AVG server to simplify SPO client maintenance and updates.

  For more information about Secure Portal Office Client, see *Avaya Configuration - Secure Portable Client Guide (NN46120-301)*.

Clientless Mode

For a partner or mobile worker to access intranet resources from any computer with Internet connectivity (an Internet caf or similar), access is made possible through the clientless mode. No manual software installation is required.

In clientless mode, interaction with the intranet is done through the web Portal through HTTP, Java Applets and ActiveX controls, which gives the client full HTTP access to the intranet. It also provides FTP and SMB (Windows file shares) access from the browser. All network traffic between the client and the VPN Gateway is sent through a secure SSL connection.

Clientless mode capabilities include intranet browsing, file server access through the Portal, Telnet/SSH access and application tunneling (port forwarding).

Web Portal

In clientless mode, the remote user connects to the VPN through the web browser. Through the web Portal, the remote user can access intranet resources from different tabs.

For a more detailed description of the Portal, see The Portal from an End-User Perspective on page 287.

Net Direct Client

Net Direct provides end-users with clientless SSL access to the intranet. By clicking a link on the Web Portal, the Net Direct client is downloaded, installed and launched on the remote user's PC. While Net Direct is running in the background, the remote user can access intranet resources through his or her native applications – without the need to install VPN client software manually.

Cached Version

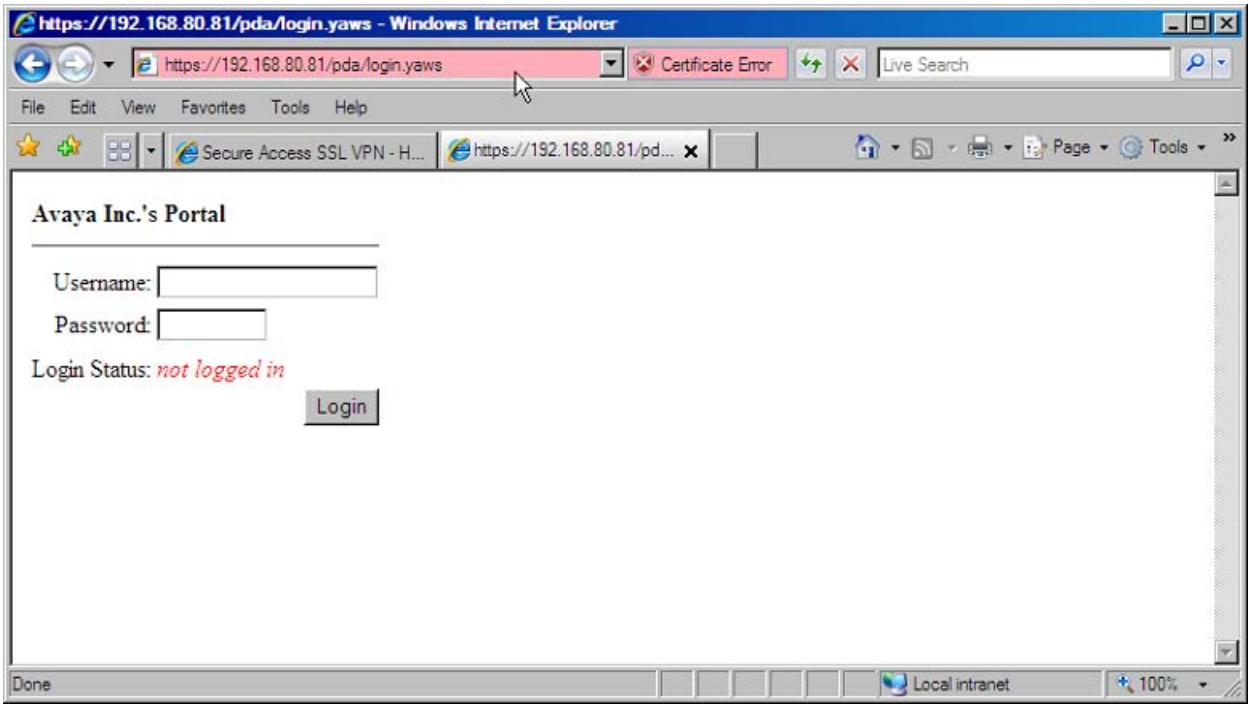
To cut down on network traffic and start-up time, a cached version of Net Direct is also available as a configurable option. If enabled, Net Direct leaves some components from the first installation on the client machine when the user exits the Portal session. These components will be only be retrieved from the server anew in the circumstance where they become outdated.

Installed Version

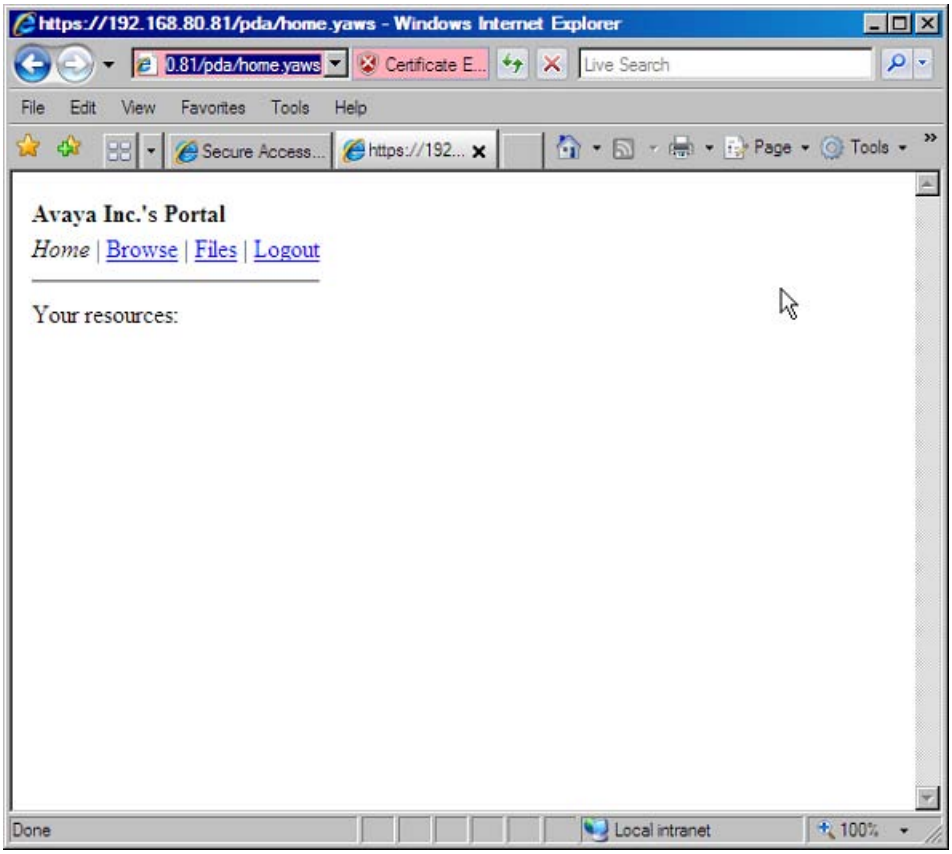
The Net Direct client is also available as a setup.exe file to be installed permanently on the remote users' machines. See Installed Version of Net Direct on page 27.

PDA Support

Clientless mode also includes PDA (Personal Digital Assistant) support. To browse to the PDA page, enter the portal address followed by /pda, for example `https://vpn.example.com/pda`. The Portal login page appears:



Once logged in, the PDA Portal appears. The PDA Portal layout is a simplified version of the web Portal. Its capabilities include intranet web browsing and file server access (only for downloading files). Change the company name if desired.



The preceding example shows the **Home** tab with two linksets with one link each.

Note:

When configuring an SMB (Windows file share) link to be displayed on a PDA Portal, specifying a shared network folder is required.

Transparent Mode

As opposed to clientless mode, transparent mode requires the user to install VPN client software, either the Avaya SSL VPN client or the Avaya VPN Client (formerly the Contivity VPN client). The VPN Gateway will then act as the VPN server.

The term "transparent" is mainly relevant from a user perspective. It means that the remote user will experience network access as if actually sitting within the corporate intranet. No Portal interaction is required. Transparent mode supports access to the intranet through legacy TCP- and UDP-based client applications.

Avaya SSL VPN Client

The Avaya SSL VPN client is permanently installed on the remote user's machine. The SSL VPN client is available in two versions:

- LSP (Layered Service Provider) client. Compatible with Windows 98, ME, NT (with IE 5 or later) 2000, and XP. This client does not support UDP.
- TDI (Transport Driver Interface) client. Compatible with Windows 2000, and XP. This client supports UDP as well as TCP. Native Microsoft Outlook is however not supported because not fully qualified domain names cannot be resolved.

The SSL VPN client is instructed to connect to the VPN Gateway and intervenes as soon as the remote user initiates a TCP or UDP connection to the intranet. Depending on the client's configuration, the request can either be directed to the VPN Gateway through a secure SSL tunnel or be directed straight to the requested destination.

For more information about the SSL VPN client, along with configuration instructions, see Transparent Mode on page 263.

Avaya VPN Client (formerly Contivity VPN Client)

The Avaya VPN Client should be installed on the remote user's machine and configured with the desired authentication option along with the IP address or domain name of the AVG cluster.

Once the VPN client is started on the remote user's machine and the user is authenticated to the VPN Gateway, requests made by the remote user are tunneled to the VPN Gateway through a secure IPsec tunnel.

For more information about the VPN client along with configuration instructions, see Transparent Mode on page 263.

Installed Version of Net Direct

As mentioned previously, the Net Direct client is also available as a setup.exe file to be installed permanently on the remote user's machines. No Portal login is required. The user logs in through the user interface provided by the installable Net Direct client.

For more information, including instructions on how to configure the Avaya VPN Gateway for use with the Net Direct client, see Net Direct on page 171.

VPN Client Summary

As mentioned previously in this chapter, the AVG software supports several types of VPN clients. The following table contains a summary of supported operating systems and protocols for available VPN clients:

VPN Client	Security Protocol	Network Protocols	Operating Systems	Requires pre-installation
Net Direct (downloadable client)	SSL	All IP protocols	Windows 2000, XP, Linux, Macintosh, Windows Vista, Windows 7 (32 bit and 64 bit).	No
Net Direct (installable client)	SSL	All IP protocols	Windows 2000, XP, Windows Vista, Windows 7 (32 bit and 64 bit).	Yes
IPsec VPN client	IPsec, SSL	All IP protocols	Windows XP, Vista, Windows 7 (32 bit and 64 bit).	Yes
SSL VPN client (LSP)	SSL	TCP	Windows 98, ME, NT (with IE 5 or later), 2000, XP, Windows 7 (32 bit and 64 bit).	Yes
SSL VPN client (TDI)	SSL	TCP/UDP	Windows 2000, XP, Windows 7 (32 bit and 64 bit).	Yes

Compatibility matrices for the AVG 9.0 are provided in the *AVG 9.0 Release Notes* (NN46120–400).

Authentication and Access Control

To achieve secure authentication and access control, the AVG can use both external authentication servers and the VPN Gateway 's built-in local database. The same mechanisms are used for both clientless and transparent mode. Authentication can also be achieved by

means of client certificate authentication. For instructions on how to configure authentication methods, see Authentication Methods on page 75.

External Database Authentication

Companies with external authentication servers (RADIUS, LDAP, NTLM, Netegrity SiteMinder, RSA ClearTrust and/or RSA SecurID) can use these servers for authentication without modification. The authentication server and fallback order is defined on the VPN Gateway.

Local Database Authentication

If no external authentication server exists, or if speedy deployment is required, the VPN Gateway can act as an authentication server itself. It can store thousands of user authentication entries each defining user name, password and the name of access groups.

Access Rules

Each user is mapped to one or more access groups stored in the AVG. The access rules associated with the group define the user's access rights to resources on the corporate intranet. The access rules permit or deny access to servers based on a combination of criteria:

- Destination host or network
- Ports or protocol
- Path (for HTTP, SMB and FTP file browsing)
- Source IP address (if extended profiles are used)
- Authentication method (if extended profiles are used)
- Access method (if extended profiles are used)
- Client PC properties (if extended profiles are used)
- Maintenance status of the VPN Gateway

If no access group is defined for a certain user a configurable default access group can be used.

In Groups, Access Rules and Profiles on page 35 you will find instructions on how to define groups, access rules and profiles.

Customize the Portal

Customize the Portal with respect to logo, language, color, static texts and so on. For instructions on how to customize the Portal, see Customize the Portal on page 197.

Configure Group-Specific Linksets

Hypertext links to intranet and Internet web pages and server applications can easily be configured. Links appear on the Portal's Home tab. Which links are displayed for the logged on user depends on the user's group membership and which linksets are mapped to the user group. For instructions on how to configure linksets and links, see Group Links on page 127.

Configure Avaya Endpoint Access Control Agent

Avaya Endpoint Access Control Agent (EACA) is an application that checks that the required components (executables, DLLs, configuration files, and so on) are installed and active on the remote user's machine. For instructions on how to configure EACA, see Configure Avaya Endpoint Access Control Agent on page 217.

Enable WholeSecurity Scan

Using the Symantec WholeSecurity Confidence Online software, a scan of client PCs can be performed before the user has actually logged on to the VPN. When the remote user connects to the VPN, he or she is automatically redirected to a WholeSecurity Confidence Online server on the intranet. The Confidence Online software is downloaded to the endpoint machine and performs a scan to identify any eavesdropping threats, including Trojan horses, remote controls, keystroke loggers and worms. See WholeSecurity on page 243.

Chapter 5: DNS Settings

This chapter describes how to configure search domains and local DNS servers.

Configure Search Domains

Search domains are automatically appended to the host names when a remote user types in the various address fields on the web Portal (if a match is found).

Example: If you specify the search domain `example.com`, a remote user can access the web page `inside.example.com` by typing `inside` in the URL field displayed on the Portal's **Home** tab.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Advanced**.
7. Click on **DNS** tab.

   The DNS form appears.
8. In the **Search List** field, enter the desired domain, for example **`example.com.`**

   If you specify more than one domain name, separate the names with a comma (,). The domains are searched in the order you specify them, and the search stops when a valid domain name is found.
9. Click **Update** and apply the changes.

Configure DNS Servers

Depending on how you wish to deploy your VPN configuration, you can either use a global DNS server (configured by your ISP) or configure the system to use your local, or private, DNS server on the intranet. If a local DNS server has been configured for your VPN, this server will be queried for DNS lookups. If not, the system's global DNS server(s) will be queried.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Advanced**.
7. Click on **DNS** tab.

   The DNS form appears.
8. Under **DNS Servers**, click **Add**.

   The DNS Settings form appears.
9. In the **New DNS IP** field, enter the IP address of your local DNS server.
10. Click **Add**.
11. Apply the changes.

Dynamic DNS Registration

The AVC sends Dynamic Domain Name System (DNS) registration messages to the DNS Server after it connects to the VPN Gateway. This can result in a number of stale DNS registrations.

The administrator can now configure whether the client will send this type of message or not.

About this task

Use the following procedure to set the registrations messages status.

Procedure

1. Navigate to the User Tunnel Configuration.`Config –> VPN gateway –> <Gateway_ID> –> IPsec –> User tunnel profiles –>`

<User_tunnel_ID>

2. Set the DNS registration state from the Client DNS Registration field pull-down menu. The options are Enabled or Disabled.

Chapter 6: Groups, Access Rules and Profiles

This chapter describes the authorization part of the AAA system, how to configure access rules and profiles for specific user groups.

When the remote user is authenticated and user's group(s) have been returned from the external authentication database (for example RADIUS), the Avaya VPN Gateway will map these group names to group names defined on the VPN Gateway. If local database authentication is used, the user's user name and password should be configured in the VPN Gateway's local database. This is also where the user is mapped to one or more groups.

For more information about selecting authentication databases and methods, see Authentication Methods on page 75.

Group Parameters

All the group members shares the limitations and capabilities that you assign to the group. The most important parameters from the group's access rules controls the authorization of a group member.

Configure the following parameters for a group:

- Linksets
- User type
- Access rules
- Default group
- Extended profiles
- Number of login sessions
- Idle timeout/Max session length
- IP pool
- Avaya Endpoint Access Control Agent rules
- IPsec tunnel access
- Avaya IE cache wiper (enable/disable)
- Citrix MetaFrame support (enable/disable)
- Net Direct (enable/disable)
- Windows admin user name/password

Linksets

Provide each with one or several linksets. The linkset itself contains one or several links. The links appear on the Portal's **Home** tab for the user to access intranet or Internet web sites, mail

servers or web applications. When a group member is logged in to the Portal, all linksets mapped to the user's group will be displayed on the **Home** tab.

Make sure the links defined for the group are not contradicted by the access rules specified for the group (see following).

For instructions on how to create linksets and links, see Group Links on page 127.

User Type

The user type determines which Portal tabs will be displayed for the user. Note that the user type distinction has no effect on access rules or vice versa.

The following user types are available:

- Novice. Displays the Home tab.
- Medium. Also displays the Files (and the Access tab if enabled).
- Advanced. Displays all tabs, which includes the Advanced tab.

For a description of the Portal, see The Portal from an End-User Perspective on page 287.

Access Rules

To be able to configure an access rule, you first have to create one or several network, service and application specific definitions. A network definition identifies hosts and/or subnets to which the user should be authorized (or unauthorized). A service definition identifies ports and/or protocols to which the user should be authorized (or unauthorized). An application specific definition identifies a path to a subfolder and/or file to which the user should be authorized (or unauthorized). The access rule is configured by referencing the desired network, service and application specific definitions in the access rule.

When the user requests a resource (for example an intranet web server), the access rules associated with the user's group are applied in order until a match is found. The system first checks Access rule 1, then Access rule 2 and so on.

If a match is found between the requested resource and the network/service/path referenced in the access rule, the action specified for the access rule is performed (accept or reject). The remaining access rules (with higher numbers) will be ignored. This means that the order in which the access rules are defined could be important. If no match is found in any access rule, the user's request is rejected.

Default Group

If a user group returned from the authentication database cannot be matched against any group configured on the Avaya VPN Gateway, the user is automatically mapped to the default group

(if configured). To create a default group, first create a group with limited access rights. Then make this group the default group. In the BBI System tree view, select **VPN Gateways** , select the name of the VPN Gateways. In VPN Summary screen, under Settings, select **Groups**. In the **Default Group** list box, select the group to be used as the default group.

Extended Profiles

Create Extended Profiles to provide better or fewer access rights to a remote user depending on

- authentication method (for example RADIUS)
- access method (SSL, IPsec or Net Direct)
- source network (for example a branch office)
- if a client certificate is used
- if the client PC has passed/failed the Avaya Endpoint Access Control Agent checks
- if the user has installed the IE cache wiper.

For instructions on how to configure extended profiles, see Working with Extended Profiles on page 54.

Number of Login Sessions

You can also define the maximum number of simultaneous Portal/VPN sessions allowed for members of a group.

Example: If the value is set to 2, two simultaneous VPN sessions (from two different computers) are allowed for a specific user.

Idle Timeout

The idle timeout for a remote user's VPN session can be configured as a default value for the whole VPN under **VPN Gateways>VPN #>General Settings**. It can also be configured on group level or, if desired, on extended profile level.

Example: If the value is set to 20m (20 minutes), the remote user is automatically logged out from the Portal session (or the VPN client session) following 20 minutes of inactivity.

Maximum Session Length

Like the idle timeout, the maximum length of a remote user's VPN session can be configured as a default value for the whole VPN under **VPN Gateways>VPN #>General Settings** It can also be configured on group level or, if desired, on extended profile level.

Example: If the value is set to 1h (1 hour), the remote user is automatically logged out from the Portal session (or the VPN client session) after 1 hour, irrespective of the user being idle or not.

IP Pool

To enable Net Direct and Avaya IPsec VPN client connections, an IP pool has to be configured, under **VPN Gateways -> VPN # -> IP Pool**. By mapping the IP pools to different user groups you can provide different ways of assigning IP address and network attributes depending on the user's group membership.

One of the configured IP pools should be selected as the default IP pool. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

For more information about IP pools, see Net Direct on page 171 and Transparent Mode on page 263.

Avaya Endpoint Access Control Agent Rules

By mapping an Avaya Endpoint Access Control Agent (EACA) SRS rule to a group, the all group members will be subject to an EACA check upon login. The SRS rule determines which software that should be present (or not present) on the client machine for the user to be granted access to the VPN.

For more information about EACA, along with configuration instructions, see Configure Avaya Endpoint Access Control Agent on page 217.

IPsec Tunnel Access

For a group member to be able to log in to the VPN with the Avaya IPsec VPN client (formerly Contivity VPN client), the group should be mapped to a previously created user tunnel profile. If group login is used, a shared secret should also be configured for the current group.

For more information about IPsec access with the Avaya IPsec VPN client, along with configuration instructions, see Transparent Mode on page 263.

Avaya IE Cache Wiper

Whether or not remote users should be able to install the Avaya IE cache wiper can be configured per VPN or per group. To delegate this setting to a per group level, select **group** in the **Use ActiveX Component for Clearing Cache** list box under **VPN Gateways -> VPN # -> Portal General**. Then enable or disable the feature in the **Wiper** list box for the desired user groups. When the IE cache wiper is enabled, the user – if running Internet Explorer – will have the option to download an ActiveX component (the Avaya IE cache wiper). The IE cache wiper removes the Portal address from the browser's visited URLs list when the Portal session is over. In addition, any HTML pages cached during the Portal session will be cleared from the cache memory.

Citrix Metaframe Support

Whether or not remote users should be able to install the Java applet supporting Citrix Metaframe web links can be configured per VPN or per group. To delegate this setting to a per group level, select **group** in the Citrix Support list box under **VPN Gateways -> VPN # -> Portal General**. Then enable or disable the feature in the **Citrix Support** list box for the desired user groups.

When enabled, a Java applet is started when users belonging to the current group logs in to the Portal. The applet enables support for Citrix Metaframe web links on the Portal. The link is created by specifying the URL to the Citrix Metaframe server with the **internal** link type.

When disabled, links to Citrix Metaframe servers are only supported if created by means of the **custom** port forwarder link type. If Citrix Metaframe links are not used, **off** is the recommended setting, because this saves the AVG from starting the Java applet.

Net Direct Access

Whether or not remote users should be able to download the Net Direct client can be configured per VPN or per group. To delegate this setting to a per group level, select **group** in the Net Direct client list box under **VPN Gateways -> VPN # -> VPN Client -> Net Direct**. Then enable or disable the feature in the **Net Direct Client** list box for the desired user groups.

For more information about the Net Direct client, along with configuration instructions, see Net Direct on page 171.

Local Administrator User Name/Password

You can also configure a common Local administrator user name/password combination for members of the current group. To be able to install the Net Direct client (downloadable from the Portal), users has to be administrator users on their PCs.

Multiple Groups

If a user belongs to several groups, the system starts by checking Group 1 (as defined on the VPN Gateway) to see if that group name matches any of the group names returned from the authentication database. It then continues with Group 2 and so on until all matches are found. A list of matching groups, reflecting the BBI/CLI order, is then maintained by the system during the user's login session.

When the user requests a resource, the access rules associated with Group 1 in this session-based list are checked in sequential order until a match is found. If a match is found, the remaining groups will be ignored. If no match is found, the access rules associated with Group 2 are checked and so on.

- Linksets: All linksets configured for the user's different groups will be displayed on the Portal's **Home** tab.
- User type. The best user type assigned to the user's different groups will be applied. This means that if the user belongs to one group configured with the novice user type and another with the advanced user type, all of the Portal's tabs will be displayed.
- Avaya Endpoint Access Control Agent SRS rules. The groups are checked in BBI configuration order. The first found SRS rule in any of the user's groups is used.
- IE cache wiper and Citrix support. Avaya IE cache wiper and Citrix Metaframe support will be enabled if it is enabled for any of the groups.
- Idle timeout and maximum session length: The highest value among the user's groups and the default value will be selected at login.

AAA Configuration Order

Following steps are required for a fully operational AAA system:

- Configure network definitions. A network definition identifies hosts and subnets to which the user should be authorized (or unauthorized). The network definition should later be referenced in an access rule. The steps are described further on in this chapter.
- Configure service definitions. A service definition identifies ports and/or protocols to which the user should be authorized (or unauthorized). The service definition should later be referenced in an access rule. The steps are described further on in this chapter.
- Configure application specific definitions. An application specific definition identifies the path to which the user should be authorized (or unauthorized). The application specific definition should later be referenced in an access rule. The steps are described further on in this chapter.
- Configure groups. If external database authentication is used, users are configured on the external authentication server along with one or several group names. The corresponding (or relevant) group names should also be configured on the VPN Gateway. If local database authentication is used, both users and groups should be configured on the VPN Gateway (see Configure users). The steps are described further on in this chapter.
- Configure access rules for the group. This is done by referencing previously created network, service and application specific definitions and setting the action to accept or reject. The steps are described further on in this chapter.
- Configure the desired authentication mechanism(s). This could be an external authentication mechanism (for example RADIUS), the VPN Gateway local database or client certificate authentication. The steps are described in Authentication Methods on page 75.
- Configure linksets with links. Linksets are displayed on the Portal's Home tab for the logged in group member. Linkset and link configuration is described in Group Links on page 127.
- Configure users. If local database authentication is used, the user should be configured on the VPN Gateway. This is also where to map the user to one or several previously defined groups. The steps are described in Authentication Methods on page 75.

Extended Profiles

If extended profiles should be applied to groups, a couple of more steps are involved. See Working with Extended Profiles on page 54 for configuration examples.

Network, Service and Path Configuration

To be able to reference a network, service or path (application specific definition) when defining the access rules for a group, you have to first configure the desired network, service and path definitions. The definitions exemplified in this section will later be referenced in access rules in the group configuration examples on Group Configuration on page 47.

Create Network Definitions

Access to Outlook Web Access Server

Use this procedure to create a network definition that identifies an Outlook Web Access server on the intranet.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Authorization**.
7. Click **Add**.

   The Add Network form appears.
8. In the **Name** field, enter a network name and click **Continue**.

   In this example we will create a network definition called owa (short for Outlook Web Access). The form is expanded to show the Network Subnets list.
9. Under **Network Subnets**, click **Add**.

   The Add Network Subnet form appears.
10. In the **New Network Address** field, enter a subnet (and netmask) identifying the Outlook Web Access server. OR Enter the OWA server's host name in the **Hostname** field.

    When creating a subnet, enter either the host name or the network address/ netmask.
11. Click **Update**.

The subnet is added to the network list.

12. Apply the changes.

Access to Intranet File Server

This procedure describes how to create a network definition identifying an intranet file server.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Authorization**.
7. Click **Add**.

   The Add Network form appears.
8. In the **Name** field, enter a network name and click **Continue**.

   In this example we will create a network definition called fileserver. The form is expanded to show the Network Subnets list.
9. Under **Network Subnets**, click **Add**.

   The Add Network Subnet form appears.
10. In the **Network Address** and **Network Mask** fields, enter a subnet (and netmask) identifying the intranet file server. OR Enter the file server's host name in the **Hostname** field.
11. Click **Update**.

    The subnet is added to the network list.
12. Apply the changes.

Access Denied to Specific Subnet

This example describes how to create a network definition identifying a specific subdomain in the company intranet to which the group members should be unauthorized. The subdomain is called secret.example.com.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.

4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Authorization**.
7. Click **Add**.

   The Add Network form appears.
8. In the **Name** field, enter a network name and click **Continue**.

   In this example we will create a network definition called secret. The form is expanded to show the Network Subnets list.
9. Under **Network Subnets**, click **Add**.

   The Add Network Subnets form appears.
10. In the **Network Address** and **Network Mask** fields, enter a subnet (and netmask) identifying the sub domain. OR Enter the sub domain's host name in the **Hostname** field.

    When creating a subnet, enter either the host name or the network address/ netmask. To specify all hosts within a sub domain, you can use an asterisk (*) as a wildcard.
11. Click **Update**.
12. Apply the changes.

    We will later reference these network definitions in different access rules in the group configuration examples starting on Group Configuration on page 47.

Create Service Definitions

Note:

If you ran the VPN Quick Setup wizard during the initial setup, 10 default service definitions were created automatically, each identifying one or several common application protocols.

Access to HTTP Protocol

This example describes how to create a service definition allowing access to the HTTP application protocol.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the system tree view, select **VPN Gateways**.

5. Select the VPN Gateway name.
6. Under **Settings**, select **Authorization**.
7. Click on **Services** tab.
8. Click **Add**.

   The Add Service form appears.
9. In the **Name** field, enter a name for the service.

   In this example we will create a service definition called http.
10. Check allowed protocols.
11. Specify allowed port numbers.

    For HTTP, enter `80`.
12. Click **Update**.
13. Apply the changes.

    We will later reference this service definition in an access rule in the group configuration examples starting on Group Configuration on page 47.

Access to FTP and SMB Protocols

This example describes how to create a service definition allowing access to the FTP and SMB (Windows file share) application protocols.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Authorization**.
7. Click on **Services** tab.
8. Click **Add**.

   The Add Service form appears.
9. In the **Name** field, enter a name for the service.

   In this example we will create a service definition called fileshare.
10. Check allowed protocols.
11. Specify allowed port numbers.

    For FTP and SMB, specify 20,21,139.

12. Click **Update**.
13. Apply the changes.

    We will later reference this service definition in an access rule in the group configuration examples starting on Group Configuration on page 47.

Create Path (Appspec) Definition

Access to Subfolder on Web Server

This example describes how to create an Appspec definition, identifying a path to a subfolder. We will later reference this Appspec definition in an access rule where the webserver network definition we created in the example on Access to Intranet File Server on page 43 will also be referenced.

The path to define in this example is`/public`. When the remote user tries to access the web server identified in the webserver network definition, the following URL will create a match: `192.168.201.10/public`.

The path setting is checked for the following protocols: HTTP, HTTPS, FTP and SMB (Windows file share). The syntax for entering the path is shown:

- For SMB, write the path as `/WORKGROUP/FILESHARE/FILE PATH`, for example `/AVAYA/homes/public`. This will give access to the public directory in the homes share in the AVAYA workgroup/domain.
- For FTP, write the path as ABSOLUTE FILE PATH, for example `/home/share/public/`. This will give access to the `/home/share/public` directory. Note that all paths are absolute from the root.
- For web servers (HTTP or HTTPS), write the path as SERVER PATH, for example `/intranet`. This will give access to the `/intranet` path on the web server.

  1. Log on as VPN portal user.
  2. Choose **Tools**, **VPN Administration**.
  3. Select **Config** tab.
  4. In the system tree view, select **VPN Gateways**.
  5. Select the VPN Gateway name.
  6. Under **Settings**, select **Authorization**.
  7. Select **Application** and click **Add**.

     The Add Application Specific Entry form appears.
  8. In the **Name** field, enter a name for the entry and click **Update**.

9. In the System tree view, under **Application**, select **Paths**.

   The Application Specific Entry Paths form appears.
10. In the **Application Group** list box, select the desired application specific entry.
11. Click **Add**.

    The Add Path form appears.
12. In the **Path** field, enter the desired path.

    In this example the path to add is `/public`.
13. Click **Update**.
14. Apply the changes.

    We will reference this appspec definition in an access rule in the group configuration examples starting on Group Configuration on page 47.

Group Configuration

This section describes how to configure a group on the VPN Gateway and gives three examples of how to define access rules for this specific group.

Example 1: Access to Specific Services on Specific Intranet Hosts

By defining the access rules described in this example, the group members will be able to access only the following intranet resources:

- Read mail through Outlook Web Access
- Browse a specific intranet web server
- Browse files on a specific file server through SMB or FTP

Configure Group 1

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Groups**.

The Groups form appears.

7. Click **Add**.

   Add a Group form appears.

8. In the **Name** field, enter a group name.

   When an external database is used for authentication (for example RADIUS), the group name assigned in the AVG configuration is matched against group names retrieved from the external authentication database.

9. In the **User Type** list box, select the desired user type.

   Assign the advanced user type to the group. This means all Portal tabs will be available to the group members.

10. Click **Update**.

    The Groups form is redisplayed with the new group added.

11. To edit the settings for the group, select the check box on the group's row and click **Edit**.

    The Group Configuration form appears.

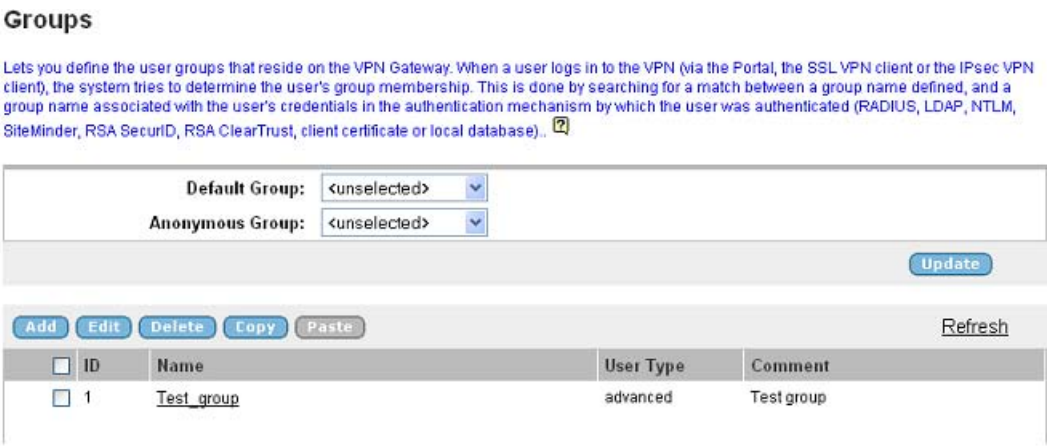
    Now the form includes additional fields, for example, for mapping an IP pool to the group and for configuring idle timeout and maximum session length. See Number of Login Sessions on page 37 and forward for explanations to available options.

12. Click **Update** and apply the changes (if any).

Configure Access Rule 1

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Groups**.

   The Groups form appears.



7. Select the desired group in the **Group** list box and click **Refresh**.
8. Click on **Access List** tab in Modify Group Name screen.
9. Click on the **Access List** tab.
10. Click **Add** to configure Access rule 1.

    The Add Rule form appears.
11. In the **Network** list box, select **owa.**

    This step lets you reference the network definition we created in the example on Access to Outlook Web Access Server on page 42, that is **owa**. It consists of a subnet definition identifying an Outlook Web Access server.
12. In the **Service** list box, select **http.**

    This step lets you reference the **http** service definition, corresponding to TCP port number 80. It limits access to the HTTP protocol.
13. Keep the asterisk (*) in the **Application** list box. This means that there are no restrictions to paths in the specified domain.
14. Finally, in the **Action** list box, select **Accept**.
15. Click **Update**.

Configure Access Rule 2

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.

6. Under **Settings**, select **Groups**.

   The Groups form appears.
7. Select the desired group in the Group list box and click **Refresh**.
8. Click on the **Access List** tab.
9. Click **Add** to configure Access rule 2.

   The Add Rule form appears.
10. In the Network list box, select **webserver**.

    This step lets you reference the network definition we created in the example on Access to Intranet File Server on page 43, that is **webserver**. It consists of a subnet definition identifying an intranet web server.
11. In the Service list box, select **http**.

    This step lets you reference the **http** service definition, corresponding to TCP port number 80. It limits access to the HTTP protocol.
12. In the Application list box, select **public**.

    This step lets you reference the application specific name we created in the example on page Access to Subfolder on Web Server on page 46. This means that group members are only allowed access to the **/public** subfolder on the web server identified by the **webserver** network definition.
13. Finally, in the Action list box, select **Accept**.
14. Click **Update**.

Configure Access Rule 3

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Groups**.

   The Groups form appears.
7. Select the desired group in the Group list box and click **Refresh**.
8. Click on the **Access List** tab.
9. Click **Add** to configure Access rule 3.

   The Add Rule form appears.

10. In the Network list box, select **fileserver**.

    This step lets you reference the network definition we created in the example on Access to Intranet File Server on page 43, that is **fileserver**. It consists of a subnet definition identifying an FTP and SMB file server.

11. In the Service list box, select **`fileshare`**.

    This step lets you reference the **fileshare** service definition (created in the example on Access to FTP and SMB Protocols on page 45), corresponding to TCP port numbers 20, 21 and 139. It limits access to the FTP and SMB protocols.

12. Keep the asterisk (*) in the Application list box. This means that there are no restrictions to paths in the specified domain.
13. Finally, in the Action list box, select **Accept**.
14. Click **Update**.
15. Apply the changes.

Example 2: Access Allowed to All Services on Hosts in a Specific Subdomain

By defining the access rules described in this example, group members will be able to access all available applications within the sales.example.com sub domain.

Access Allowed to Specific Subnet

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Groups**.

   The Groups form appears.

7. In the **Group** list box, select the user access group for which the access rule should be applied and click **Refresh**.
8. Click on the **Access List** tab.
9. Click **Add**.

   The Add Rule form appears.

10. In the Network list box, select **sales**.

11. Keep the asterisks (*) in the Service and Application list boxes. This implies all port numbers, protocols and paths.
12. In the Action list box, select **Accept**.
13. Click **Update**.
14. Apply the changes.

Example 3: Access Allowed to the Complete Intranet, Except for Hosts in a Specific Subdomain

By defining the access rules described in this example, group members will be able to access all intranet resources except for all hosts in the secret.example.com sub domain, regardless of the protocol used.

Note:

Remember that when a match is found for a requested resource, the action specified for the matching resource in an access rule is performed (accept or reject), and access rules with a higher number are ignored. Therefore, it is extremely important that the access rule that rejects access to all hosts within the secret.example.com subdomain in this example is defined as access rule number 1.

Access Rule 1: Access Denied to Specific Subdomain

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Groups**.

   The Groups form appears.
7. In the **Group** list box, select the user access group for which the access rule should be applied and click **Refresh**.
8. Click on the **Access List** tab.
9. Click **Add**.

   The Add Rule form appears.
10. In the **Network** list box, select **secret**.

This step lets you reference the secret network definition (see Access Denied to Specific Subnet on page 43).

11. Keep the asterisks (*) in the Service and Application list boxes. This implies all port numbers, protocols and paths.
12. In the **Action** list box, select **reject**.
13. Click **Update**.
14. Apply the changes.

Access Rule 2: Access Allowed to All Hosts

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Groups**.

   The Groups form appears.
7. In the and **Group** list box, select the user access group for which the access rule should be applied and click **Refresh**.
8. Click on the **Access List** tab.
9. Click **Add**.

   The Add Rule form appears.
10. Keep the asterisks (*) in the Network, Service and Application list boxes. This implies all networks, port numbers, protocols and paths.
11. In the **Action** list box, select **Accept**.
12. Click **Update**.
13. Apply the changes.

Creating a VPN Administrator Account

This section describes the steps to enable/disable the right to configure the Avaya VPN Gateway device from the Browser-Based Management Interface (BBI) for members of the current group. Follow these steps, for the VPN Admin configuration:

1. Create a VPN X using Console connection or through BBI from Clean Side with group trusted (Group 1).
2. Load SSP License
3. Enable VPN Administration for VPN X.
4. Enable VPN Administration for group trusted (Group 1) as shown in the following figure.

5. Apply the configuration.

   Therefore, the users who come under group trusted (Group 1) now have the provision to perform vpn specific configuration by logging into the portal.

Working with Extended Profiles

Specifying access rules on Group level (as described in the previous sections in this chapter) is sufficient to have a working AAA system. However, if security considerations in your company require a more fine-grained authorization control, one or more extended profiles can be added to a user group.

In short, extended profiles are used to give the remote user better or fewer access rights depending on how the user's accesses the VPN.

Base Profiles and Extended Profiles

Define all the data for a group on Group level (access rules, linksets, user type and so on.) can also be defined for an extended profile. Data defined on Group level, that is. directly under the Group menu, adhere to the group's base profile. Data defined on the Extended profile menu adhere to the group's extended profile.

When is the Extended Profile Applied?

The client filter referenced in the extended profile determines when the extended profile's access rules should be applied.

The client filter identifies

- the source network (for example a branch office)
- the authentication method (for example RADIUS)
- the access method (for example SSL, IPsec or Net Direct)
- if a client certificate is installed on the remote user's machine
- whether or not the Avaya Endpoint Access Control Agent checks have failed
- if the IE cache wiper is installed on the remote user's machine.

When the user is authenticated, the system starts by checking Extended profile 1 to see if a match can be found between the client filter conditions and the user's security status.

If no match is found in Extended profile 1, the system goes on to check Extended profile 2 for a matching client filter and so on. When a match is found, that particular extended profile's data (access rules, linksets and so on) will be applied. Data defined for the base profile will be appended to the extended profile's data. If no match in any of the extended profiles, only the base profile's data will be applied.

Linksets

Which linksets to be displayed on the Portal for the logged in group member can for example be determined by the user's source network or authentication method. For example, if an extended profile references a source network that is considered secure, this profile could provide another set of links than the base profile. The base profile's linksets are however appended to the extended profile's linksets.

Access Rules

Which access rules should apply during the currently logged in group member's session is also determined by the extended profile. For example, the access rules defined for an extended profile that references a secure access method could be more generous. Like with linksets, the base profile's access rules are appended to those of the extended profile.

The extended profile's access rules are executed prior to those of the base profile. This means that if a match is found in any of the extended profile's access rules (for example the access rule's network definition matches the user's requested network), the action specified for the

access rule (for example accept) will be performed. The base profile may contain an access rule with the same network definition, but this access rule will be ignored.

User Type

Where user type is concerned, the best user type assigned to the user group's extended profile and base profile will be applied. This means that if the extended profile has the novice user type assigned to it and the base profile uses the advanced user type, the advanced user type will be applied, that is. all of the Portal's tabs will be displayed for the logged in user.

Multiple Groups

If a user belongs to several groups, the system starts by checking Group 1 (as defined on the VPN Gateway) to see if that group name matches any of the group names returned from the authentication database. It then continues with Group 2 and so on until all matches are found. A list of matching groups, reflecting the CLI order, is then maintained by the system during the user's login session.

Where profiles are concerned, each group is treated separately by the system. The extended profile(s) associated with Group 1 are first checked in sequential order to see if a match can be found between the user's security level (for example source network) and the client filter referenced in the extended profile. If a match is found, the extended profile's access rules and linksets will be applied and the base profile's data will be appended.

The system continues to check Group 2 for extended profiles in the same way. If no match is found in an extended profile, the base profile will be used. The system then checks Group 3. If a match is found in an extended profile, this profile's access rules and links will be applied and the base profile's access rules and links will be appended. This means that several extended and base profiles may be active at the same time for the logged in user.

Using the preceding example, the following access rules could be valid during a session for a logged in user that belongs to Group 1, Group 2 and Group 3:

Table 1: Valid Access Rules for a User that Belongs to Multiple Groups

Group 1	Group 2	Group 3
Extended profile 1 (no match)	Extended profile 1 (no match)	Extended profile 1 (match)
Extended profile 2 (match)	Extended profile 2 (no match)	
Base profile	Base profile	Base profile
Result: The access rules of Extended profile 2 and the base profile will be valid for the user's current session.	Result: Only the base profile's access rules will be valid for the user's current session.	Result: The access rules of Extended profile 1 and the base profile will be valid for the user's current session.

When the user requests a resource, for example an intranet host, the system will first check the access rules that are valid for Group 1. The extended profile's access rules are checked prior to the base profile's access rules.

If no match is found between the user's request and the network, services and so on specified in Group 1's access rules, the system goes on to check Group 2, that is only the base profile's access rules in this example. If a match is found in any of Group 2's access rules, the access rules pertaining to Group 3 will be ignored. If no match is found in Group 2, the system goes on to check the access rules valid for Group 3.

To avoid the complexity of overlapping access rules when multiple access groups are configured, we recommend that each individual group's access rules cover separate areas.

Example 1: Define the Staff Group

In this example, we will create a group called staff. The base profile should include a link to an Outlook Web Access server and an access rule that allows access to that OWA server. Access to the OWA server should be allowed, regardless of whether the user requests the server from an Internet caf or from a secure network.

We will also add an extended profile to the staff group. The extended profile references a client filter which, in its turn, references a client network. The client network consists of a subnet identifying a secure network, that is a branch office. When a group member connects to the SSL VPN from the branch office network over the internet, that group member should have more generous access rights.

Define the Base Profile

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Groups**.
7. Click **Add**.

   The Add New Group form appears.
8. In the **Name** field, enter the group name.

   In this example, enter the name staff.
9. In the **User Type** list box, select the desired user type.

   Select **Advanced** as user type.

10. Click **Update**.
11. In the tree view, select **VPN Gateways**.
12. Select the VPN Gateway name.
13. Under **Settings**, select **Groups**.
14. In the **Group** list box, select the user access group for which the access rule should be configured. Click **Refresh**.
15. Click **Edit**.
16. Click on the **Access List** tab.
17. Click **Add**.

    The Add Rule form appears.

    The next step is to specify the access rule pertaining to the base profile.
18. In the **Network** list box, select **owa**.

    This step lets you reference the network definition we created in the example on Access to Outlook Web Access Server on page 42, i.e owa. It consists of a subnet definition identifying an Outlook Web Access server.
19. In the Service list box, select **http**.

    This step lets you reference the http service definition, corresponding to TCP port number 80. It limits access to the HTTP protocol.
20. Keep the asterisk (*) in the Application list box.

    This implies all paths in the specified domain.
21. In the Action list box, select **Accept**.
22. Click **Update**.

Define a Link for the Base Profile

This example shows how to create a linkset with a link to the Outlook Web Access server. The link will be displayed on the Portal's **Home** tab for the logged on group member.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Portal Linksets**
7. In the System tree view, select **VPN Gateways**.

8. Select the VPN Gateway name.

   VPN Summary screen appears.

9. Under **Settings**, select **Linksets**.

   The Portal Linksets form appears.

10. Click **Add**.

    The Add New Linkset form appears.

11. In the **Name** field, enter the name **owa**.

    We will later map this linkset name to the staff group.

12. In the **Text** field, enter a heading for the linkset (optional).

    The linkset heading is displayed above the links in the linkset.

13. Click **Update**.

14. In the System tree view, under Portal Linksets, select **Links**.

    The Portal Links form appears.

15. In the **Portal Linkset** list box, select the linkset where the new link should be included. Click **Refresh**.

16. Click **Add**.

    The Add Portal Links form appears.

17. In the **Text** field, enter the clickable link text that will show up on the Portal's Home tab under the portal link heading (if configured).

    Enter **E-mail** as the link text.

18. In the **Link Type** list box, select the desired link type, in this case Internal Website.

    For a full reference to all available link options, see Group Links on page 127.

19. Click **Continue**.

    The Internal Website Links form appears.

20. Under **Internal Link Settings**, in the **Protocol** list box, select **http**.

21. In the **Host** field, enter the host name of the OWA server.

22. In the **Path** field, enter a forward slash (/).

23. Click **Update**.

Map the Linkset to the User Group

The link will not be displayed for the group member unless the linkset we have just created is mapped to the desired user group.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Linksets**.

   The Portal Linksets form appears.
7. Click **Add**.
8. In the **Name** field, enter the name `owa`.

   We will later map this linkset name to the staff group.
9. In the **Text** field, enter a heading for the linkset (optional).

   The linkset heading appears above the links in the linkset.
10. Click **Update**.
11. Apply the changes.

Create a Network Identifying the Branch Office Network

To be able to reference the client network in the client filter, you should first create the network definition identifying the branch office network.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Authorization**.
7. Under Networks form, click **Add**.

   The Add Network form appears.
8. In the **Name** field, enter the network name.

In this example we will call the network branchoffice.

9. Click **Continue**.

   The form is expanded.

10. Under Network Subnets, click **Add**.

    The Add Network Subnet form appears.

11. In the Hostname field, enter the address of the branchoffice network, in this example *.denver.example.com.

    This step creates the subnet to be included in the network definition. When creating a subnet, enter either the host name or the network address/netmask. To specify all hosts within a sub domain, you can use an asterisk (*) as a wildcard.

12. Click **Update**.
13. Apply the changes.

Define a Client Filter Referencing the Client Network

To be able to reference the client filter in the extended profile, you have to first define the client filter.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under Settings, select **Authorization**.
7. Click on **Filters** tab.

   Client Filters form appears.

8. Under Client Filters form, click **Add**.

   Add Client Filter form appears.

9. In the Name field, enter the client filter's name.

   In this example we will call the filter branchoffice.

10. Click **Update**.
11. Apply the changes.

Define the Extended Profile and Client Filters

To be able to reference the client filter in the extended profile, you have to first define the client filter.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.

   VPN Summary screen appears.
3. Under **Settings**, select **Groups**.

   The Client Filters form appears.
4. Click on **Extended Profile**.

   The Extended Profiles form appears.
5. Click **Add**.

   The Client Filters are added to the table.
6. Click on the **Modify** button in the table.
7. Click on the **Access List** tab.

   Extended Access List form appears.
8. Click **Add**.

   The Add Rule form appears for you to specify Access rule 1, allowing access to all networks and protocols.
9. Keep the asterisk (*) in the Network, Service and Application list boxes. This implies all networks, services and paths.
10. In the **Action** list box, select **Accept**.
11. Click **Update**.

Note:

Leaving an extended profile without access rules is not the same as denying all traffic. If no access rule at all is specified for the extended profile, the base profile's access rules will be applied.

Create a Linkset with a Link to an FTP File Server

This linkset belongs to the extended profile. The linkset defined for the base profile will be appended to this linkset, that is both linksets will be displayed for group members accessing the Portal from the branch office network.

For a full reference to all available linkset and link options, see Group Links on page 127.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Linksets**.

   The Portal Linksets form appears.
7. Click **Add**.

   The Add New Linkset form appears.
8. In the **Name** field, enter the name `ftp`.
9. In the **Text** field, enter a heading for the linkset (optional).

   The linkset heading is displayed above the links in the linkset.
10. In the System tree view, under Portal Linksets, select **Portal Links**.

    The Portal Links form appears.
11. Click **Add**.

    The Add Portal Links form appears.
12. In the **Text** field, enter the clickable link text that will show up on the Portal's Home tab under the portal link heading (if configured).

    Enter `FTP file server` as the link text.
13. In the **Link Type** list box, select the desired link type, in this case FTP.

    For a full reference to all available link options, see Group Links on page 127.
14. Click **Continue**.

    The Portal Links form is expanded.
15. Under **FTP Link Settings**, in the FTP host field, enter the IP address or hostname of the FTP server.

    In this example we will enter the host name `ftp.example.com`.
16. In the **Initial Path on Host** field, enter `/!` to specify the home directory.
17. Click **Update**.

Map the Linkset to the Extended Profile

The next step is to map the linkset to the extended profile we created for the staff group.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.

   VPN Summary screen appears.
3. Under **Settings**, select **Groups**.

   The Client Filters form appears.
4. Click on **Extended Profile**.

   The Extended Profiles form appears.
5. Click **Add Profile**.

   The extended profile is added to the table.
6. Click on the Modify button in the table.
7. Click on the **Access List** tab.

   Extended Access List form appears.
8. In the **Group** list box, select the desired user access group and click Refresh.
9. In the **Client Filter** list box, select the client filter (identifying the extended profile) to which the linkset should be mapped.
10. In the **Portal Linksets** list box, select the portal linkset that you wish to map to the current extended profile.
11. Click **Add**.
12. Apply the changes.

Result

Bill is a member of the staff group. This is what will happen depending on how Bill accesses the Portal:

- From an Internet caf: The extended profile will not be triggered. This is because the client filter referenced in the extended profile points to the branch office network, not the Internet caf 's network. Only the linkset mapped to the base profile (that is directly under Groups in the System tree view) will be displayed on the Portal's Home tab. If Bill tries to access the Outlook Web Access server, either by clicking the link or by entering the address in the **Home** tab's URL field, access will be allowed. A match will be found between the requested resource and the network referenced in Access rule 1. If Bill tries to request any other resource, no match will be found in the access rule and access will be denied.
- From the branch office network: The extended profile will be triggered. This is because a match is found between Bill's source network and the client network referenced in the extended profile's client filter. Both linksets will be displayed, because the base profile's linksets are always appended to those of the extended profile. The access rule defined for the extended profile will be applied, which means Bill is granted access to all hosts

and protocols on the intranet and the internet. The base profile's access rule will be appended but has no real effect in this example.

Example 2: Define the Engineer Group

In this example, we will create a group called engineer. The base profile should contain a link to an intranet web server and an access rule that allows access to all hosts in the sales.example.com subdomain.

Members of the engineer group exist in the VPN Gateway local database as well as in a RADIUS authentication server's database. Thus, group members can authenticate to the Portal using local database authentication or RADIUS authentication. The latter is considered more secure.

For users logging in to the Portal using local database authentication, only the base profile's links and access rules should be applied. The Advanced tab should not be visible on the Portal. For users logging in to the Portal using RADIUS authentication, links and access rules defined for the extended profile should be applied. The extended profile should contain an extra set of links, an access rule that allows access to all hosts and a user type allowing display of all of the Portal's tabs.

Define the Base Profile

This example describes how to configure the **engineer** group with the required links and access rules.

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN Gateway name.
3. Under **Settings**, select **Groups**.

   The Groups form appears.
4. Click **Add**.

   The Add New Group form appears.
5. In the **Name** field, enter a name for the group.

   In this example, name the group **engineer**.
6. In the **User Type** list box, select **medium** as user type.

   By setting the user type to medium, the Advanced tab will not be visible on the Portal for the logged in group member.
7. Click **Update**.

Configure the Base Profiles Access Rules

1. Log on as VPN portal user.
2. Under **Tools**, select **VPN Administration**
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under Settings, select **Groups**.

   The Groups form appears.
7. Click on the **Access List** tab.
8. Click **Add**.

   The Add rule form appears.
9. In the Network list box, select the **sales** network definition.
10. Keep the asterisk (*) in the Service and Application list boxes. This implies all services and paths.
11. In the Action list box, select **Accept**.
12. Click **Update**.

Create a Linkset with a Link to the Intranet Web Server

1. Log on as VPN portal user.
2. Under **Tools**, select **VPN Administration**
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under Settings, select **Linksets**.

   The Portal Linksets form appears.
7. Click **Add**.

   The Add New Linkset form appears.
8. In the **Name** field, enter the name **intranet**.
9. In the **Text** field, enter a heading for the linkset (optional).

   The linkset heading is displayed above the links in the linkset.

10. In the System tree view, select **VPN Gateways**.
11. Click on the VPN Gateway name.
12. Under **Settings**, select **Linksets**.
13. Click on the **Portal Links** tab and click **Add**.

    The Add Portal Links form appears.
14. In the **Text** field, enter the clickable link text that will show up on the Portal's Home tab under the portal link heading (if configured).

    Enter `Link to web server` as the link text.
15. In the **Link Type** list box, select the desired link type, in this case Internal Website.

    For a full reference to all available link options, see Group Links on page 127.
16. Click **Continue**.

    The Portal Links form is expanded.
17. Under Internal Link Settings, in the Protocol list box, select the desired protocol, in this example http .
18. In the **Host** field, enter `inside.example.com` as the web server's address.
19. In the **Path** field, enter forward slash (`/`) as the path to imply the web server's root.
20. Click **Update**.

Map the Linkset to the Base Profile

1. Log on as VPN portal user.
2. Under **Tools**, select **VPN Administration**
3. Click **Config** tab.
4. In the system tree view, select **VPN Gateways**.
5. Select the VPN Gateway name.
6. Under **Settings**, select **Linksets**.

   The Portal Linksets form appears.
7. In the Portal Linksets list box, select the linkset you wish to map to the group.

   In this example we will map the **intranet** linkset to the **engineer** group.
8. Click **Add**.
9. Apply the changes.

Configure RADIUS Authentication

For instructions on how to configure RADIUS authentication on the VPN Gateway, see the section RADIUS Authentication on page 77 in Authentication Methods on page 75.

Configure the Extended Profile and Client Filters

To grant members of the **engineer** group better access rights when using RADIUS authentication, we should add an extended profile to the group. The extended profile should be triggered when a group member authenticates through RADIUS, supplied by the RADIUS server. Reference the client filter we created in the example in the previous section.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.

   VPN Summary screen appears.
3. Under Settings, select **Groups**.

   The Client Filters form appears.
4. Click on **Extended Profile**.

   The Extended Profiles form appears.
5. Click **Add Profile**.

   The extended profile is added to the table.
6. Click on the **Modify** button in the table.
7. Click on the **Access List** tab.

   Extended Access List form appears.
8. In the **Group** list box, select the desired user access group and click **Refresh**.
9. In the **Client Filter** list box, select the client filter (identifying the extended profile) to which the linkset should be mapped.
10. In the **Group** list box, select the user access group for which you wish to create an extended profile.
11. Click **Refresh**.
12. In the Client Filter list box, select **`radius`** .

    This is the client filter we created in the previous section.
13. Click **Add**.

14. Under User Type, verify that the current extended profile is assigned the user type advanced. If not, select the check box (next to radius in the following example) and click **Edit** to access a form where the user type can be changed.

    The base profile's user type is **medium**. To provide better access rights for users authenticating through RADIUS, specify **advanced** as user type.

15. Click **Update**.

Configure Access Rules for the Extended Profile

This step lets you specify the group member's access rights when the user authenticates through RADIUS. The group members should be granted access to hosts on all networks. All services should be available.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.

   VPN Summary screen appears.

3. Under Settings, select **Groups**.

   The Client Filters form appears.

4. Click on **Extended Profile**.

   The Extended Profiles form appears.

5. Click **Add Profile**.

   The extended profile is added to the table.

6. Click on the **Modify** button in the table.
7. Click on the **Access List** tab.

   Extended Access List form appears.

8. In the Group list box, select the desired user access group and click **Refresh**.
9. In the Client Filter list box, select the client filter (identifying the extended profile) for which you wish to configure access rules and click Refresh.
10. Click **Add**.

    The Add Rule form appears.

11. Keep the asterisk (*) in the Network, Service and Application list boxes. This implies all networks, services and paths.
12. In the Action list box, select **Accept**.
13. Click **Update**.
14. Apply the changes.

Create and Map Linksets to the Extended Profile.

Linksets mapped to the extended profile will be displayed when the user authenticates through RADIUS. Linksets mapped to the base profile will be appended to those of the extended profile.

For a full reference to all available linkset and link options, see Group Links on page 127.

Result

Lisa is a member of the engineer group. This is what will happen depending on how Lisa authenticates to the Portal.

- Local database authentication. The extended profile will not be triggered, because Lisa authenticated to the Portal through local database authentication. Only the base profile will be used in Lisa's session. The linkset mapped to the base profile will be displayed on the Portal's Home tab. If Lisa tries to access a host within the sales.example.com sub domain, for example by entering the address in the **Home** tab'>s URL field, access will be allowed. A match will be found between the requested resource and the network referenced in Access rule 1. If Lisa tries to request any other host, access will be denied.
- RADIUS authentication. The extended profile will be triggered, because Lisa authenticated to the Portal through RADIUS database authentication. Any linksets mapped to the extended profile will be displayed on the Portal's **Home** tab. The base profile's linkset will also be displayed, because the base profile's linksets and access rules are always appended to the extended profile. The access rule defined for the extended profile will be applied, which means Lisa is granted access to all hosts and protocols on the intranet and the internet.

Note:

If a match for the requested resource cannot be found in any of the access rules defined for the extended profile, the access rules of the base profile will be applied in sequential order.

Extended Profile for Users with Client Certificate

The two previous examples describe how to create extended profiles for remote users connecting from a secure network and through a secure authentication method.

In the same way, an extended profile could be created for users with a valid client certificate installed. Because client certificate authentication is considered more secure, the extended profile could provide more generous access rules.

Configure a Group with Access Rules

These access rules should be configured directly under the Group level, thus constituting the base profile. The access rules will apply to remote users without a client certificate and should grant access to less resources than the extended profile.

Configure a Client Filter

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.

   VPN Summary screen appears.
3. Under Settings, select **Authorization**.
4. Click on **Filters** tab.

   The Client Filters form appears.
5. Click **Add**.

   Add Client Filter form appears.
6. In the **Name** field, enter a name for the client filter, for example clientcert.
7. In the **Client Cert** list box, select **true**.
8. Click **Update**.

Configure a Client Filter and Extended Profile

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.

   VPN Summary screen appears.
3. Under **Settings**, select **Groups**.
4. Click on the group name.
5. Click on **Extended Profile**.

   The Extended Profiles form appears.
6. Click **Add Profile**.

   The extended profile is added to the table.
7. Click on the **Modify** button in the table.

8. Click on the **Access List** tab.

   Extended Access List form appears.
9. In the **Group** list box, select the group for which an extended profile should be created and click **Refresh**.
10. In the **Client Filter** list box, select the client filter we created in the previous section.
11. Click **Add**.
12. In the tree view, expand **Extended Profile** and select **Extended Access List**.

    The Extended Access List form appears.
13. In the **Group** list box, select the desired user access group. and click **Refresh**.
14. In the **Client Filter** list box, select the client filter (identifying the extended profile) we created in steps 1-6.
15. Click **Add** to configure access rules for the extended profile.

    These access rules will apply to users authenticating with a client certificate.
16. Click **Update**.
17. Apply the changes.

Extended Profile for Users with IE Cache Wiper

To make sure that sensitive information is not left in the computer's cache memory after a Portal session, a user group can be configured to reject access to certain intranet resources if the remote user is not running the IE cache wiper. On the other hand, an extended profile (with more generous access rules) could be created for those who actually run the IE cache wiper.

When a user – if running Internet Explorer – logs in to the Portal from a computer for the first time, he is asked whether or not to install the IE cache wiper. The IE cache wiper clears the cache from HTML pages accessed during a Portal session. In addition, the Portal address is removed from the browser's visited URLs list.

Configure a Group with Access Rules

These access rules should be configured directly under the Group level, thus constituting the base profile. The access rules will apply to users without the IE cache wiper running and should grant access to less resources than the extended profile.

Configure a Client Filter and Extended Profile

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.

   VPN Summary screen appears.
3. Under **Settings**, select **Groups**.

   The Client Filters form appears.
4. Click on **Extended Profile**.

   The Extended Profiles form appears.
5. Click **Add Profile**.

   The extended profile is added to the table.
6. Click on the **Modify** button in the table.
7. Click on the **Access List** tab.

   Extended Access List form appears.
8. In the **Group** list box, select the group for which an extended profile should be created and click **Refresh**.
9. In the **Client Filter** list box, select the client filter we created in the previous section.
10. Click **Add**.
11. In the tree view, expand **Extended Profile** and select **Extended Access List**.

    The Extended Access List form appears.
12. In the **Group** list box, select the desired user access group. and click **Refresh**.
13. In the **Client Filter** list box, select the client filter (identifying the extended profile) we created in steps 1-6.
14. Click **Add** to configure access rules for the extended profile.

    These access rules will apply to users authenticating with a client certificate.
15. Click **Update**.
16. Apply the changes.

Extended Profile for Users with Specific Access Method

A client filter can also identify the remote user's access method, that is SSL, IPsec, Net Direct or a combination of these access methods. Configuration is done in the same way as described

for the other client filter examples in this chapter. Only select the desired access method in the Client filter form when configuring the filter.

- SSL refers to access through the Portal or the installable Avaya SSL VPN client (not the Net Direct client).
- IPsec refers to access through the Avaya IPsec VPN client (formerly Contivity).
- Net Direct refers to access through the Net Direct client.

For more information about the Avaya IPsec VPN client and the installable Avaya SSL VPN client see Transparent Mode on page 263. For more information about the Net Direct client, see Net Direct on page 171.

Extended Profile for Users that are Subject to an Avaya Endpoint Access Control Agent Check

For a detailed description of how Avaya Endpoint Access Control Agent is configured, along with examples on how to configure extended profiles, see Configure Avaya Endpoint Access Control Agent on page 217.

Chapter 7: Authentication Methods

This chapter describes how to select an authentication method for the VPN, and how to configure the settings of a particular method. After having configured the desired authentication methods, you should also specify in which order the authentication methods should be applied when a remote user logs in to the VPN.

External Database Authentication

The following external database authentication methods are supported:

- RADIUS
- LDAP
- NTLM
- Netegrity SiteMinder
- RSA SecurID
- RSA ClearTrust

When a remote user wants to access a resource provided in the VPN, the Avaya VPN Gateway authenticates the user by sending a query to an external RADIUS, LDAP, NTLM domain, Netegrity SiteMinder, RSA ClearTrust or RSA SecurID server. This makes it possible to use already existing authentication databases within the intranet. The VPN Gateway includes username and password in the query and requires the name of one or more access groups in return. The name of the LDAP and RADIUS access group attribute is configurable.

You can configure more than one authentication method within any given VPN.

Local Database Authentication

The AVG device can also act as an authentication database itself. It can store thousands of user authentication entries each defining a user name, password, and the relevant access groups. This local authentication method can be useful if no external authentication databases exist, for testing purposes or if speedy deployment is needed. The local database authentication method can actually be used as a fallback to external database queries. If for example a query to an LDAP server fails the VPN Gateway can query its own database. This comes handy if a client is to gain access to corporate resources for only a limited time.

Local database authentication is described on Local Database Authentication on page 119.

Client Certificate Authentication

With client certificate authentication enabled on the VPN Gateway, no Portal login is required for remote SSL users with a valid client certificate installed on their computers. Once the VPN Gateway has accepted the certificate, the user is directed straight to the Portal's Home tab.

With a signed client certificate imported to the remote user's Windows machine, Avaya IPsec VPN client (formerly Contivity) users can authenticate to the VPN through client certificate authentication once the client certificate has been selected in the IPsec VPN client.

Client certificate authentication is described on Client Certificate Authentication.

Login Service List Box

To support redirection to a specific authentication server, for example for token login or for redirection to a specific Windows domain, the authentication method can be assigned a display name. This name (for example SafeWord) will be selectable in the Login Service list box on the Portal login page and in the Avaya SSL VPN client login window, directing the user straight to the proper server for authentication. If the user selects **default** in the Login Service list box, authentication will be carried out according to the configured authentication order.

Secondary and Two Factor authentication

When assigning authentication servers, you have the option to specify a second authentication server to use after the first one succeeds. With this option you enable both SSL Secondary authentication and IPsec Two Factor authentication.

The secondary authentication method is a feature primarily designed to support single-sign on to backend servers in cases where the first authentication method is token-based or uses client certificate authentication. You can use only RSA, SecurID, RADIUS and client certificate authentication mechanisms for a secondary authentication server. In IPsec Two Factor authentication the client provides both the username and password to the requesting server while in SSL Secondary authentication the client needs to provide only the password. Configuring a new certificate authentication server automatically supports IPsec Two Factor authentication. IPsec Two Factor authentication supports only certificate authentication as primary servers and local, RADIUS or LDAP as secondary servers.

Note:

- To ensure SSL Secondary authentication works concurrently with IPsec Two Factor authentication, add the user ID from the certificate to the second authentication server
- To ensure that IPsec Two Factor authentication works concurrently with SSL Secondary authentication, manually add the user ID from the certificate when configuring a primary IPsec Two Factor authentication server

You can enable both SSL Secondary authentication and IPsec Two Factor authentication by selecting a secondary server from the **Secondary Authentication Server** list found in the VPN Gateways, <VPN Gateway name>, Authentication, <Authentication server name>, **Advanced** tab whenever you are adding or editing authentication servers.

RADIUS Authentication

The RADIUS authentication method lets you configure user authentication through an existing intranet RADIUS server. The RADIUS method supports Challenge/Response as well as token login methods such as SecurID, SafeWord, and ActivCard.

Configure Basic Settings

1. Log on as VPN portal user.
2. Under **Tools**, select **VPN Administration**
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example radius.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see Groups, Access Rules and Profiles on page 35.
10. In the **Display Name** field (optional), set the desired display name.

The display name will appear in the Login Service list box on the Portal login page and in the Avaya SSL VPN client's login window. This is a way of directing the remote user to the proper authentication server, if the Portal uses different authentication methods.

If the user selects **default** in the Login Service list box on the Portal login page, authentication will be carried out according to the configured authentication order.

11. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.

    This step lets you specify an NTLM domain name that can be used in automatic login links (that is iauto, or Internal Auto Login URL), where the target backend server requires a Windows domain. The <*var:domain*> macro (if included in a link) expands to the domain name specified with this command.

    For more information about this link type, see Group Links on page 127.

12. Select the authentication mechanism "radius" from drop-down list.
13. Click **Update**.

Configure RADIUS Specific Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to12 on page 79

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server appears.

8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.

10. Enter the Display name for the server.

    This is an optional field.

11. Select **radius** in **Mechanism** drop-down list.

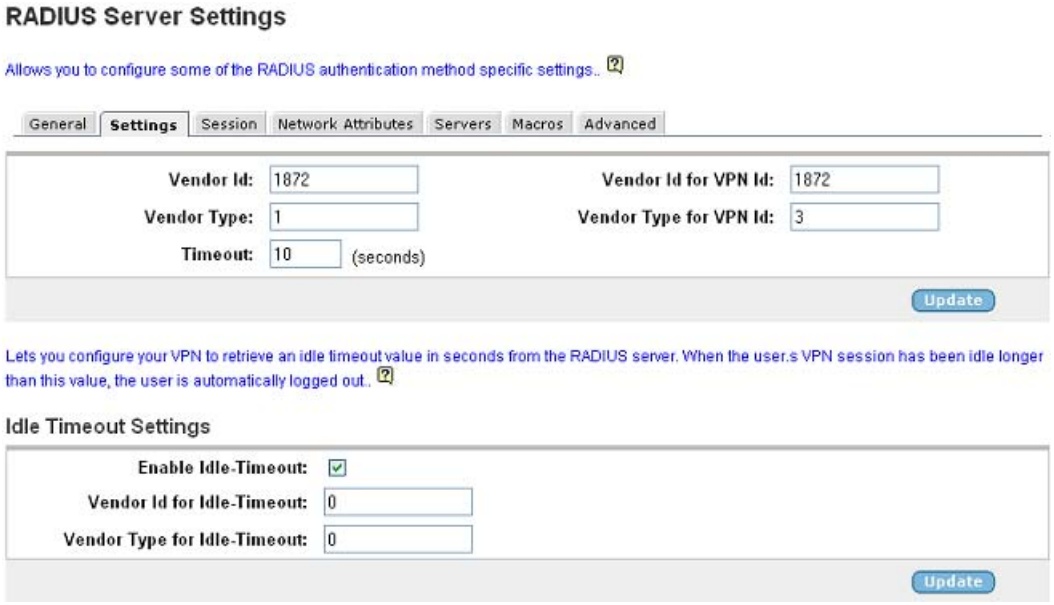
12. Click **Update**.

    A new authentication ID is created.

13. Click on the Authentication ID in Authentication Server screen.

14. Click on **Settings** tab.

    RADIUS Server Settings form appears.



15. In the **Vendor Type** field, enter the Vendor-Type value for the group attribute.

    The vendor type value is set to 1 (alteon-xnet-group) by default. If your RADIUS server uses another Vendor-Type number, you can change this value.

    Contact your RADIUS server administrator for more information. Used in combination with the Vendor-Id number, the Vendor-Type number identifies the group in which users who should be allowed access to the VPN through RADIUS authentication are members. The group name(s) to which the vendor specific attribute points must be defined in the VPN, complete with one or more access rules.

16. In the **Vendor Id for VPN Id** field, specify the Vendor-ID for the VPN ID attribute.

    This attribute is set to 1872 (alteon) by default. When a user authenticates to a specific VPN (as configured on the AVG), the AVG sends the VPN ID to the RADIUS server. The RADIUS server in its turn can make use of the VPN ID to return user information (for example from a VPN-specific user database). The Vendor-Id should correspond to the Vendor-Id used by your RADIUS server. If your RADIUS server uses another Vendor-Id, you can change this value. Contact your RADIUS server administrator for more information.

17. In the **Vendor Type for VPN Id** field, specify the Vendor-Type value for the VPN ID attribute.

    The vendor type value is set to 3 by default. If your RADIUS server uses another Vendor-Type number, you can change this value. Contact your RADIUS server administrator for more information. Used in combination with the Vendor-Id, the Vendor-Type number identifies the VPN to which the remote user has logged in.

18. In the **Timeout** field, change the RADIUS timeout value if desired.

    The default timeout value in seconds for a connection request to a RADIUS server is 10 seconds. If the timeout value elapses before a connection is established, authentication will fail.

19. Under **Idle Timeout Settings**, specify the desired Vendor-ID and Vendor-Type for the idle timeout attribute (optional).

    This step lets you configure your VPN to retrieve an idle timeout value in seconds from the RADIUS server. When the user's VPN session has been idle longer than this value, the user is automatically logged out.

    To disable retrieval of the idle timeout value from RADIUS, deselect the **Enable Idle-Timeout** check box.

20. Click **Update**.

Add RADIUS Server(s)

This step adds a RADIUS server that will be queried to perform authentication of a remote user prior to accessing resources on the Portal.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 12 on page 81.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server appears.

8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.

10. Enter the Display name for the server.

    This is an optional field.

11. Select radius in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.

13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Servers** tab and Click **Add**.

    Add New RADIUS Server form appears.

15. In the **IP address** field, enter the IP address of the RADIUS server.
16. In the **Port** field, change the default port number if desired.

    Port number 1812 is the default number but it can be changed if the RADIUS server uses another port number for the specified service.

17. In the **Shared Secret** fields, enter a unique shared secret (password).

    The shared secret is used to authenticate the VPN Gateway to the RADIUS server. Contact your RADIUS server administrator to obtain the shared secret.

18. Click **Update**.
19. Apply the changes.

Configure Network Attributes

For Net Direct and IPsec VPN client connections, client IP address and network attributes can be retrieved from a RADIUS server. This requires that your ISP has configured the VPN with an IP pool whose pool mechanism is set to radius. Contact your ISP if you have questions regarding IP address and network attributes assignment for your VPN.

If your VPN is configured to retrieve IP address and network attributes from a RADIUS server, specify the required Vendor-Id and Vendor-Type values.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.

6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 82.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server appears.

8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.

10. Enter the Display name for the server.

    This is an optional field.

11. Select **radius** in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.

13. Click on the Authentication ID in Authentication Server screen.
14. Click on the **Network Attributes** tab.

    Network Attributes Settings screen appears.

    The default Vendor-Id and Vendor-Type settings for retrieval of network attributes are displayed. If your RADIUS server uses other values for Vendor-Id and Vendor-Type, you can change the values. Contact your RADIUS server administrator for more information.

15. Click **Update** and apply the changes (if any).

Configure RADIUS Session Timeout

These steps (optional) lets you configure your VPN to retrieve a value in seconds from the RADIUS server. This value controls the length of a remote user's VPN session. Whether the user is idle or not has no effect on the session time-out. When the time is up, the user is automatically logged out.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.

6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 83.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server appears.

8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.

10. Enter the Display name for the server.

    This is an optional field.

11. Select **radius** in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.

13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Session** tab.

    RADIUS Session Settings screen appears.

15. In the **Session Timeout** list box, select **enabled.**
16. In the **Vendor ID** field, enter the Vendor-ID attribute.

    Contact your RADIUS system administrator for information about which attribute to use.

17. In the **Vendor Type** field, enter the Vendor-Type value.

    Contact your RADIUS system administrator for information about which value to use.

18. Click **Update**.

RADIUS Macro Configuration

These steps (optional) lets you add macros for creating user-specific links on the Portal's Home tab. This is done by mapping a macro to a RADIUS user attribute. When the remote user is successfully logged in, the macro will expand to the value retrieved from the logged in user's RADIUS attribute.

Example: Map an arbitrary variable name (for example exchangeServer) to a RADIUS user attribute identifying an Exchange server. Create an Internal Website link and specify the variable in the link properties, for example `http:// <var:exchangeServer> /`

`exchange/ <var:user>`. Even if different Exchange servers are used in your company, one link will be sufficient.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 84.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server appears.
8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.
10. Enter the Display name for the server.

    This is an optional field.
11. Select radius in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Macros** tab and then click on **Add**.
15. In the **Variable Name** field, enter a name of your own choice, for example `exchangeServer`. By mapping the variable name to the RADIUS attribute, the corresponding value can be retrieved from the logged in user's user record in RADIUS.
16. In the **Vendor ID** field, enter the desired Vendor-ID attribute.

    This step lets you specify the Vendor-Id number to be used when retrieving the value from the user record. Contact your RADIUS system administrator for information about which attribute to use.
17. In the **Vendor Type** field, enter the Vendor-Type value.

This step lets you specify the Vendor-Type number that identifies the user attribute whose value should be retrieved. Contact your RADIUS system administrator for information about which value to use.

18. In the **Attribute Type** list box, select the type of value to be retrieved.
19. Click **Update** and apply the changes.

Specify the Authentication Fallback Order

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.
7. Click on **Authentication Order** tab.

   The AuthOrder form appears.
8. Under **Fallback Order**, in the **Available list**, select **1 radius.**
9. Click **>>** to move the item to the Selected list.

   To change the authentication order (if several authentication IDs have been configured), move all authentication IDs back to the Available list. Then move them back one at a time to the Selected list in the order that you wish authentication to be carried out.
10. Click **Update**.
11. Apply your changes.

    When a match of user name and password is found, the other specified authentication methods (if any) in the Authentication Order list are ignored.

LDAP Authentication

The LDAP authentication method lets you configure authentication towards an existing intranet LDAP server. The LDAP method also supports some advanced Active Directory features (for example bookmarks and password expiry check) that are currently not supported by the NTLM authentication scheme.

Configure Basic Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication screen screen appears.
8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.
10. Enter the Display name for the server.

    This is an optional field. The display name will appear in the Login Service list box on the Portal login page, in the SSL VPN client's login window and in the Net Direct client's login window. This is a way of directing the remote user to the proper authentication server, if the Portal uses different authentication methods. If the user selects default in the Login Service list box on the Portal login page, authentication will be carried out according to the configured authentication order.
11. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.

    This step lets you specify an NTLM domain name that can be used in automatic login links (that is iauto, or Internal Auto Login URL), where the target backend

server requires a Windows domain. The macro <var:domain> (if included in a link) expands to the domain name specified with this command.

12. Select **LDAP** in **Mechanism** drop-down list.

    Add New LDAP Server screen appears.

13. Click **Resolve IP**.

    Add New LDAP Server screen appears.

    Entries defined in the during the creation of LDAP server is displayed in this screen.

14. Specify the iSD Bind Password and enable LDAPS.
15. Click **Update**.

Configure LDAP Specific Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 87.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.

8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.

10. Enter the Display name for the server.

    This is an optional field.

11. Select **LDAP** in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.

13. Click on the Authentication ID in Authentication Server screen.

14. Click on **Settings** tab.

    The LDAP Server Settings form appears.

15. In the **Search Base Entry** field, specify the desired search base entry.

    This step assigns the DN (Distinguished Name) that points to the entry that is one level up from where all user entries are found.

    Example of search base syntax: `ou=people,dc=foo,dc=com`

    Note:

    If user entries are located in several different places in the LDAP Dictionary Information Tree (DIT) or if the user's Portal login name is not identical with the user record identifier (RDN), a DN pointing to an entry from where the entire DIT can be searched should be assigned. This however requires the VPN Gateway to authenticate to the LDAP server, using the values specified for **isdBindDN** and **isdBindPassword** . Also see example on Search the LDAP Dictionary Information Tree (DIT) on page 97.

16. In the **Group Attribute** field, specify the LDAP group attribute name.

    This step defines the LDAP attribute that contains the group names of which a particular user is a member. The group names in the LDAP attribute must be defined for the VPN on the VPN Gateway, complete with one or more access rules. If you specify more than one group attribute name, separate the names using comma (,).

17. In the **User Attribute** field, specify the LDAP user attribute name.

    This step defines the LDAP attribute that contains the user names. The default user attribute name is uid.

18. In the **iSD Bind DN** field, specify the isdBindDN entry (optional).

    This step points out an LDAP entry (distinguished name) to which the VPN Gateway should authenticate. Normally, this step (and iSD Bind Password) can be skipped. It is only required if the VPN Gateway should authenticate to the LDAP server, for example to be able to search the Dictionary Information tree (DIT). See example on Search the LDAP Dictionary Information Tree (DIT) on page 97.

19. If required, check the **Enable LDAPS** check box.

    If checked, LDAP requests between the VPN Gateway and the LDAP server will be made using a secure SSL connection, that is LDAPS.

20. In the **Server Timeout** field, change the LDAP timeout value if desired.

    The default timeout value in seconds for a connection request to an LDAP server is 5 seconds. If the timeout value elapses before a connection is established, authentication will fail.

21. In the **User Preferences** list box (optional), select **enabled** to enable storage of user preferences in an external LDAP/Active Directory database.

    If enabled, the VPN Gateway can save user preferences accumulated during a Portal session in the **isdUserPrefs** attribute. The next time the user successfully logs in through the Portal, the VPN Gateway retrieves the LDAP attribute that holds the user preference data from the LDAP database.

    In the current version, Portal bookmarks and HTTP auto-login information is saved as user preference data.

    To support storage/retrieval of user preferences, the LDAP server needs to extend its schema with one new ObjectClass and one new Attribute. How this is done is described in Appendix H in the *User's Guide*.

22. In the **Cut Domain from User Name** list box (optional), make the desired setting.

    - enabled:

      Strips the domain part from the login user name before LDAP authentication is performed.

      Example: If the login user name is `john@example.com`, the `@example.com` part will be cut off before LDAP authentication takes place.

    - disabled:

      The domain name will not be cut off.

23. In the **Extra Search Filter** list box, select the desired option.

    If enabled, you can configure the desired attribute/value when searching for a user record in an LDAP/Active Directory database (see 24 on page 89 and 25 on page 89). The feature is disabled by default, which means that no extra requirement is added when searching for a user record.

24. In the **Extra Search Filter Attribute** field, enter the desired attribute.

    This step can be skipped the extra search filter is disabled (see 23 on page 89).

    Sets the desired attribute when searching for user records. User records that contain this attribute and the value specified in the **Extra Search Filter Attribute Value** field will be found.

    The default attribute is **objectclass.**

25. In the **Extra Search Filter Attribute Value** field, enter the desired value.

    This step can be skipped the extra search filter is disabled (see 23 on page 89).

    Sets the desired value when searching for user records. User records that contain the attribute specified in the **Extra Search Filter Attribute** field and this value will be found.

    The default value is person.

26. In the **Short Group Format** list box (optional), select **enabled** if you wish to enable extraction of group names according to the short group format.

    This step lets you configure the AVG to extract the first part of a returned Distinguished Name (DN) as the group name to be used. This makes it easier to configure the group name in the VPN as you do not have to configure the entire DN string as group name.

    - true:

      Enables extraction of the first part of the DN as group name.

      Example: If the DN reads `cn=My Group,cn=User,dc=Company,dc=com`, `"My Group "` will be used as group name.

    - false:

      The entire DN string has to be configured as group name in the CLI if returned as group name from the authentication server.

27. Click **Update**.

Configure Active Directory Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 91.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.
10. Enter the Display name for the server.

    This is an optional field.
11. Select **LDAP** in **Mechanism** drop-down list.

12. Click **Update**.

    A new authentication ID is created.

13. Click on the Authentication ID in **Authentication Server** screen.

14. Click on **Active Directory** tab.

    The LDAP Active Directory Settings form appears.

15. To enable an expired account/password check, select **enabled** in the Expired Account Check list box.

    If enabled, the system will perform an expired account/password check against Active Directory when the remote user logs in. If the account or password has expired, you can specify a group in which the user should be placed.

    The purpose of placing the user in a new group is to direct the user to a web page where the account/password can be renewed.

    When the user logs on (when authenticated through LDAPS) with an expired password they are directed to a password change page. From there, they can either change their password, or click Cancel or No to skip the password change. If the user skips the password change page, they will placed into the expired Expired Password Group. They can return to the password change page and change their password at any time from the portal. You can monitor whether or not a user has skipped the password change page using “$change_pass_op” (false means the user has skipped the page).

    First, create a user access group on the VPN Gateway in which remote users with expired accounts or passwords should be placed (can be different groups). This user group (or groups) should have access to the web server hosting the account/password renewal site. Configure an access rule for the group, restricting access to the specified site.

    Then configure a linkset including a link to the account/password renewal site and map the linkset to the group. Finally specify the group name(s) in the **Expired Account Group** and **Expired Password Group** fields in this form.

    For instructions on how to create user access groups, see Groups, Access Rules and Profiles on page 35.

16. Select the desired group in the **Expired Account Group** list box.

    This step sets the group in which users with expired accounts should be placed.

17. Select the desired group in the **Expired Password Group** list box.

    This step sets the group in which users with expired passwords should be placed.

18. In the **Password expiration Pop-up Warning** list box, select whether or not to display a popup warning window when the password is about to expire.

19. In the **Recursive Group Membership** list box, select the desired option.
    - enabled:

      If the remote user belongs to an Active Directory group which, in its turn, belongs to another group, all groups are returned.
    - disabled:

      If the remote user belongs to an Active Directory group which, in its turn, belongs to another group, only the first group is returned.
20. Click **Update**.

Configure Group Search Settings

This step lets you configure the AVG to find group information about an iPlanet Directory Server.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 92.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.
10. Enter the Display name for the server.

    This is an optional field.
11. Select LDAP in Mechanism drop-down list.
12. Click **Update**.

    A new authentication ID is created.
13. Click on the Authentication ID in Authentication Server screen.

14. Click on **Group Search** tab.

    The LDAP Group Search Settings form appears.

15. In the **Group Search** list box, select enabled to enable the group search feature.

16. In the **Group Search Base Entry** field, specify the desired Distinguished Name (DN).

    This step assigns the DN (Distinguished Name) that points to the entry where to start searching for group entries in the Dictionary Information Tree (DIT) on the iPlanet Directory Server.

    Example: `ou=groups,dc=avaya,dc=com`

    Once the logged in user's credentials have been verified against a user record on the iPlanet Directory server, the system uses the user's DN to search for the user's groups. When a group member attribute whose value matches the user's DN is found, the group entry DN is returned as the group name.

    The group entry DN could for example be `cn=Staff,ou=groups=,dc=avaya,dc=com`. This would however be quite a long group name to configure in the VPN. To simplify configuring group names in the VPN, enable the **Authentication>LDAP>LDAP Settings (Short Group Format)** setting (see 26 on page 90). Using the preceding example, the group name Staff can then be extracted from the group entry DN.

17. In the LDAP Group Member Attribute field, enter the desired group member attribute.

    This step defines the LDAP attribute that contains the group member's name. The default value is uniqueMember.

18. Click **Update**.

Configure LDAP Server(s)

This step adds an LDAP server that will be queried to perform authentication of a remote user prior to accessing resources on the Portal.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 94.

Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.

8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.

10. Enter the Display name for the server.

    This is an optional field.

11. Select **LDAP** in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.

13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Servers** tab and Click **Add**.

    The Add New LDAP Server form appears.

15. In the **IP address** field, enter the LDAP server's IP address.
16. In the **Port** field, enter the port number to be used.

    Port number 389 is the default number but it can be changed. If LDAPS (LDAP over SSL) should be used for traffic sent between the VPN Gateway and the LDAP server, port number 636 should be used.

17. Click **Update** and apply the changes.

LDAP Macro Configuration

These steps (optional) lets you add your own macros, for example to create user-specific links on the Portal's Home tab. This is done by mapping a variable (or macro) of your own choice to an LDAP user attribute. When the remote user is successfully logged in, the variable will expand to the value retrieved from the logged in user's LDAP attribute.

Example: Map an arbitrary variable name (for example exchangeServer) to an LDAP user attribute identifying an Exchange server. Create an internal link and specify the variable in the link properties, for example `http:// <var:exchangeServer> /exchange/ <var:user>`. Even if several different Exchange servers are used in your company, one link will be sufficient.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.

3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 95.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.
10. Enter the Display name for the server.

    This is an optional field.
11. Select **LDAP** in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Macros** tab and then click on **Add**.

    The Add New User-defined Macro form appears.
15. In the **Variable Name** field, enter a name of your own choice, for example exchangeServer.

    By mapping the variable name to the LDAP attribute, the corresponding value can be retrieved from the logged in user's LDAP/Active Directory user record.
16. In the **LDAP Attribute** field, enter the desired LDAP attribute.

    This step sets the LDAP user attribute whose value should be retrieved.
17. In the **Prefix** field (optional), enter the desired prefix.

    This is useful if the LDAP attribute's value string is long and you wish to extract the value following the prefix. Combine with a suffix if the value is in the middle of the string.
18. In the **Suffix** field (optional), enter the desired suffix.

This is useful if the LDAP attribute's value string is long and you wish to extract the value preceding the suffix. Combine with a prefix if the value is in the middle of the string.

19. Click **Update** and apply the changes.

Specify the Authentication Fallback Order

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.
7. Click on **Authentication Order** tab.

   The AuthOrder form appears.
8. Under **Fallback Order**, in the **Available** list, select **2 ldap.**
9. Click **>>** to move the item to the Selected list.

   To change the authentication order (if several authentication IDs have been configured), move all authentication IDs back to the Available list. Then move them back one at a time to the Selected list in the order that you wish authentication to be carried out.
10. Click **Update**.
11. Apply your changes.

    When a match of user name and password is found, the other specified authentication methods (if any) in the Authentication Order list are ignored.

Search the LDAP Dictionary Information Tree (DIT)

Searching the LDAP Dictionary Information Tree (DIT) is necessary if

- user entries are located in several different places in the DIT
- if the user's Portal login name is not identical with the user record identifier (RDN) on the LDAP server.

The following example shows the adjustments that have to be made to the LDAP configuration if the user's Portal login name is not identical with the user record identifier (RDN) on the LDAP server.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 97.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter the Authentication server name.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used.
10. Enter the Display name for the server.

    This is an optional field.
11. Select LDAP in **Mechanism** drop-down list.
12. Click **Update**.

    A new authentication ID is created.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Settings** tab.

    The LDAP Server Settings form appears.
15. In the **Search Base Entry** field, set the LDAP searchbase entry.

Example of search base syntax: `ou=people,dc=foo,dc=com`

16. In the **User Attribute** field, set the LDAP user attribute name, for example `sAMAccountName.`

    In this example, the user's portal login name is not identical with the user record identifier (RDN). To find the user record in the LDAP Dictionary Information Tree (DIT), a combination of the user's login name and a user attribute will be used when searching the tree.

    In Active Directory, the sAMAccountName attribute contains the value that corresponds to the user's login name. Thus, if the user's login name is bill, the user record will be found because it matches the sAMAccountName attribute value for the user whose record identifier (RDN) is cn=bill smith.

17. In the **iSD Bind DN** field, point out an LDAP entry (distinguished name) to be used for AVG authentication.

    To be able to search the DIT, the VPN Gateway must authenticate itself towards the LDAP server.

18. In the **iSD Bind Password** field, set a password for AVG authentication.

    This step sets the password to be used when the VPN Gateway authenticates itself to the LDAP entry pointed out with the **`isdbinddn`** command.

19. Click **Update**.

20. Apply your changes.

NTLM Authentication

The NTLM authentication method lets you configure authentication towards a Windows server, Samba or Novell server. The NTLM method works with Active Directory, but if more advanced AD features like bookmarks and password expiry checks are desired, you should use the LDAP authentication method instead (see LDAP Authentication on page 86).

Configure Basic Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.

6. Under settings, select **Authentication**.

   Authentication Server screen is displayed.

7. Click **Add**.

   Add New Authentication server is displayed.

8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example ntlm.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see Groups, Access Rules and Profiles on page 35.

10. In the **Display Name** field (optional), set the desired display name, for example if you have multiple NTLM domains.

    The display name will appear in the Login Service list box on the Portal login page and in the SSL VPN client's login window. This is a way of directing the remote user to the proper authentication server, if the Portal uses different authentication methods.

    By selecting **default** in the Login Service list box on the Portal login page, authentication will be carried out according to the configured authentication order.

11. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.

    This step lets you specify an NTLM domain name that can be used in automatic login links (that is iauto, or Internal Auto Login URL), where the target backend server requires a Windows domain. The <*var:domain*> macro (if included in a link) expands to the domain name specified with this command.

    For more information about this link type, see Group Links on page 127.

12. Select **ntlm** in **Mechanism** drop-down list.

    To be able to specify another server for group information retrieval, you have to configure this authentication server with an authentication ID of its own.

13. Click **Update**.

NTLM Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.

5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 100.

   Authentication Server screen is displayed.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.

   This step sets the group in which the remote user should automatically be placed if the user's NTLM password has expired.

   First, define the user group on the AVG. Create a linkset with a link to a site where the user can change his/her NTLM password. Map the linkset to the group. Also remember to configure an access rule restricting access to the specified site.
9. In the **Name** field, enter a name for the authentication method, for example ntlm.
10. Enter the display name of the server.
11. Select ntlm in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Settings** tab.

    The NTLM Server Settings form appears.
15. In the **Password Expired Group** list box (optional), enter the desired user access group.

    This step sets the group in which the remote user should automatically be placed if the user’s NTLM password has expired. First, define the user group on the AVG. Create a linkset with a link to a site where the user can change his/her NTLM password. Map the linkset to the group. Also remember to configure an access rule restricting access to the specified site.
16. Click **Update**.

Add NTLM Server(s)

This step adds an NTLM server that will be queried to perform user authentication.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.

5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under **settings**, select **Authentication**. If Authentication server is already present go to 13 on page 101.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.

   This step sets the group in which the remote user should automatically be placed if the user's NTLM password has expired.

   First, define the user group on the AVG. Create a linkset with a link to a site where the user can change his/her NTLM password. Map the linkset to the group. Also remember to configure an access rule restricting access to the specified site.
9. In the **Name** field, enter a name for the authentication method, for example `ntlm`.
10. Enter the display name of the server.
11. Select ntlm in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Servers** tab and Click **Add**.

    The Add New NTLM Server form appears.
15. In the **IP address** field, enter the IP address of the NTLM server.
16. Click **Update** and apply the changes.

Specify the Authentication Fallback Order

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.

5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.
7. Click on **Authentication Order** tab.

   The AuthOrder form appears.
8. Under **Fallback Order**, in the **Available** list, select **2 ntlm**.
9. Click **>>** to move the item to the Selected list.

   To change the authentication order (if several authentication IDs have been configured), move all authentication IDs back to the Available list. Then move them back one at a time to the Selected list in the order that you wish authentication to be carried out.
10. Click **Update**.
11. Apply your changes.

    When a match of user name and password is found, the other specified authentication methods (if any) in the Authentication Order list are ignored.

SiteMinder Authentication

To configure the AVG to use a Netegrity SiteMinder policy server for user authentication is fairly easy. On the other hand, a great deal of configuration is required on the SiteMinder side. The VPN Gateway acts as a client, or agent, to the SiteMinder server. Therefore, the VPN Gateway should be configured as an agent in SiteMinder.

This manual assumes that you are familiar with SiteMinder or have access to SiteMinder documentation.

Note:

SiteMinder authentication cannot be configured for VPNs that are bound to a specific interface. Binding VPNs to interfaces are typically used in a Secure Service Partitioning configuration, that is when the VPN is provided to an end-customer by an Internet Service Provider (ISP).

Configure Basic Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.

5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server is displayed.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example siteminder.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see Groups, Access Rules and Profiles on page 35.
10. In the **Display Name** field (optional), set the desired display name.

    The display name will appear in the Login Service list box on the Portal login page and in the SSL VPN client's login window. This is a way of directing the remote user to the proper authentication server, if the Portal uses different authentication methods.

    By selecting **default** in the Login Service list box on the Portal login page, authentication will be carried out according to the configured authentication order.
11. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.

    This step lets you specify an NTLM domain name that can be used in automatic login links (that is iauto, or Internal Auto Login URL), where the target backend server requires a Windows domain. The <*var:domain*> macro (if included in a link) expands to the domain name specified with this command.

    For more information about this link type, see Group Links on page 127.
12. In the **Group Authentication Servers** list, you can specify that another authentication server should be used for retrieving group information (optional).

    Group information can only be retrieved from the Local database and LDAP databases. LDAP variables (if configured) are also retrieved. If user groups exist in the current authentication scheme, these will be added to the user groups found in the referenced authentication scheme(s).

    To be able to specify another server for group information retrieval, you have to configure this authentication server with an authentication ID of its own.
13. Click **Update**.

Configure SiteMinder Specific Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 104.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example **`siteminder`**.
10. Enter the display name of the server.
11. Select **siteminder** in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Settings** tab.

    The SiteMinder Server Settings form appears.
15. In the Failover Mode list box, define the mode for accessing the SiteMinder authentication servers.

    This setting does only apply if several SiteMinder servers are configured.

    In roundrobin mode, the VPN Gateway will connect to the SiteMinder servers on a turn basis, that is the first connection request is directed to the SiteMinder server configured with index number 1, the second to the server configured with index number 2 and so on.

    In failover mode, if the SiteMinder server configured with index number 1 fails, the VPN Gateway will connect to the server configured with index number 2.

    The default mode need not normally be changed.
16. In the **Group Attribute** field, enter the attribute that identifies the Agent Type Attribute defined in SiteMinder.

When creating the Agent Type in SiteMinder, the Agent Type Attribute identifier must be equal to this value. The default group attribute is 64.

17. In the **AgentName** field, define the name of the agent, that is the VPN Gateway.

    The VPN Gateway will function as the agent, or client, to SiteMinder. An agent with this exact name must be also configured in SiteMinder.

    The default agent name is Avaya Agent.

18. In the **Timeout** field, change the SiteMinder timeout value if desired.

    The default timeout value in seconds for a connection request to a SiteMinder server is 5.

19. In the **Secret** fields, enter a unique shared secret (password) that the VPN Gateway will use to authenticate to the SiteMinder server.

20. To enable single sign-on for remote users having authenticated to another SiteMinder server in the same domain, select **true** in the Allow Single Sign-On list box.

    This feature configures the VPN Gateway to automatically log in a remote user to the VPN if the user has a valid SMSESSION cookie from another SiteMinder-enabled site. This works as long as the VPN (for example `vpn.example.com`) and the other SiteMinder-enabled site (for example `a.example.com`) are on the same DNS domain. The SiteMinder session will however be invalidated when the user logs out from the Portal, if `/cfg/vpn #/server/portal/wipecookie` is set to `on` (default value).

    If the remote user logs in to `vpn.example.com` without a valid SMSESSION cookie, the VPN Gateway will set the SMSESSION cookie as a domain cookie. This way the user can auto-log in to `a.example.com`. The SiteMinder session will however be invalidated if the user logs out from the Portal.

    Note:

    If Single Sign-On is set to true but no display name or authentication order is configured for the SiteMinder authentication method on the VPN Gateway, it will not be possible to log in to the VPN without a valid SMSESSION cookie.

21. In the Resource field (optional), enter the desired path.

    Sets the path to a protected resource that is also defined in SiteMinder.

22. If Single-Sign-On is set to **`true`**, set the desired scope in the Domain Cookie Scope field.

    This setting determines the value of the domain cookie when Single Sign-On is enabled (see previous step).

Example:

- `0:` The most specific domain name will be calculated from the host name. If the Portal's host name is `a.b.c.d.e`, the domain cookie's value will be `.b.c.d.e`.
- `3:` If the Portal's host name is `a.b.c.d.e`, the domain cookie's value will be `.c.d.e`.
- `2`: If the Portal's host name is `a.b.c.d.e`, the domain cookie's value will be `.d.e`.

The scope must be either `0` or greater than or equal to `2`.

23. Click **Update**.

Add SiteMinder Server(s)

This step adds a SiteMinder server that will be queried to perform user authentication.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 106.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example **`ntlm`**.
10. Enter the display name of the server.
11. Select siteminder in **Mechanism** drop-down list.
12. Click Update.
13. Click on the **Authentication ID** in Authentication Server screen.
14. Click on **Servers** tab and click **Add**.

    The Add New SiteMinder Server form appears.
15. In the **IP Address** field, enter the IP address of the SiteMinder server.

16. Verify that the suggested port numbers in the Port number fields are correct.
17. Click **Update** and apply the changes.

Specify the Authentication Fallback Order

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.
7. Click on **Authentication Order** tab.

   The AuthOrder form appears.
8. Under **Fallback Order**, in the **Available** list, select **2 siteminder**.
9. Click **>>** to move the item to the Selected list.

   To change the authentication order (if several authentication IDs have been configured), move all authentication IDs back to the Available list. Then move them back one at a time to the Selected list in the order that you wish authentication to be carried out.
10. Click **Update**.
11. Apply your changes.

    When a match of user name and password is found, the other specified authentication methods (if any) in the Authentication Order list are ignored.

RSA ClearTrust Authentication

Besides installing the ClearTrust components on the desired machines in your network, you should also configure the VPN Gateway to act as a ClearTrust web server and point out configured ClearTrust dispatcher(s) or authorization server(s).

The VPN Gateway sets a ClearTrust single-sign-on cookie in the client browser. This means that the user does not have to log in once again if requesting a password-protected web page on a ClearTrust-aware backend server. The cookie is automatically validated against the ClearTrust authorization server.

This manual assumes that you are familiar with ClearTrust or have access to ClearTrust documentation. The following instructions describe the configuration required on the VPN Gateway.

Configure Basic Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server is displayed.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example cleartrust.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see Groups, Access Rules and Profiles on page 35.
10. In the **Display Name** field (optional), set the desired display name.

    The display name will appear in the Login Service list box on the Portal login page and in the Avaya SSL VPN client's login window. This is a way of directing the remote user to the proper authentication server, if the Portal uses different authentication methods.

    By selecting **default** in the Login Service list box on the Portal login page, authentication will be carried out according to the configured authentication order.
11. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.

    This step lets you specify an NTLM domain name that can be used in automatic login links (that is iauto, or Internal Auto Login URL), where the target backend

server requires a Windows domain. The <*var:domain*> macro (if included in a link) expands to the domain name specified with this command.

For more information about this link type, see Group Links on page 127.

12. In the Group Authentication Servers list, you can specify that another authentication server should be used for retrieving group information (optional).

    Group information can only be retrieved from the Local database and LDAP databases. LDAP variables (if configured) are also retrieved. If user groups exist in the current authentication scheme, these will be added to the user groups found in the referenced authentication scheme(s).

    To be able to specify another server for group information retrieval, you have to configure this authentication server with an authentication ID of its own.

13. Click **Update**.

Configure ClearTrust Settings

The ClearTrust Server Settings form includes a number of default settings that normally need be changed.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 109.

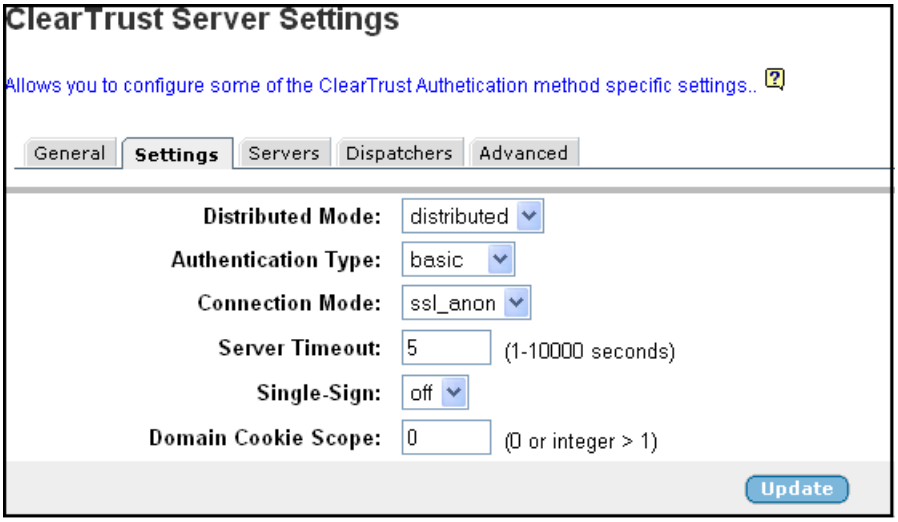
   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.

8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example cleartrust.
10. Enter the display name of the server.
11. Select cleartrust in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Settings** tab.

The ClearTrust Server Settings form appears.



15. In the **Distributed Mode** list box, select the desired option.

    This step sets the desired connection mode for the ClearTrust web server agent, that is the VPN Gateway.

    - standard:

      The AVG sends requests to the first available ClearTrust authorization server.

    - distributed:

      The AVG distributes requests among all available ClearTrust authorization servers. It first chooses the server with the least number of outstanding packets. Where all servers are equal in outstanding packets, it picks the server with lowest average response time. Under low loads, a fraction of the requests are distributed randomly among eligible servers to keep the response time estimates updated and select faster servers.

16. In the **Authentication Type** list box, select the desired option.

    This step sets the desired authentication type for the ClearTrust web server agent (that is the VPN Gateway).

    - basic:

      Basic authentication validates the User ID and password provided at login with the user account information in the RSA ClearTrust data store. This is the default authentication type for all RSA ClearTrust-protected resources and to enable it requires no additional setup tasks.

    - nt:

Enables NT authentication. NT authentication is handled by the ClearTrust authorization server and requires server-side configuration. See the RSA ClearTrust documentation for instructions.

- securid:

  Enables RSA SecurID two-factor authentication to validate a username and passcode at login against the credentials stored in the RSA ACE/Server. A passcode is a combination of a user's PIN and RSA SecurID valid token code entered as one continuous string. If the passcode is valid, the RSA ACE/Server returns the request to the RSA ClearTrust authorization server for access control checking. See the RSA ClearTrust documentation for additional information about how to enable SecurID authentication for a web server agent.

17. In the **Connection Mode** list box, select the desired option.

    This step sets the desired connection type for the ClearTrust web server agent (the VPN Gateway) when connecting to other RSA ClearTrust components.

    - clear:

      Data sent between the ClearTrust components is not encrypted.

    - ssl_anon:

      Data sent between the ClearTrust components is encrypted using anonymous SSL, that is neither the client nor the server is required to present a certificate to authenticate itself. A tunnel is set up between communicating servers, using 128-bit encryption. When this option is selected, all the RSA ClearTrust components (the ClearTrust Servers and Agents) must be configured to use anonymous SSL.

18. In the **Server Timeout** field, enter the desired value.

    This step sets a timeout value in seconds for a connection request to a ClearTrust server. If the timeout value elapses before a connection is established, authentication will fail. The default value is 5 seconds.

19. Specify whether or not SSO (single sign-on) should be allowed.

    If set to **on**, the VPN Gateway is configured to automatically log in a remote user to the VPN if the user has a valid CTSESSION cookie from some other ClearTrust-enabled site. This works as long as the VPN (for example `vpn.example.com`) and the other ClearTrust-enabled site (for example a`.example.com`) are on the same DNS domain. The ClearTrust session will however be invalidated when the user logs out from the Portal, if `/cfg/vpn #/server/portal/wipecookie` is set to `on` (default value).

    If the remote user logs in to `vpn.example.com` without a valid CTSESSION cookie, the VPN Gateway will set the CTSESSION cookie as a domain cookie. This

way the user can auto-log in to a `.example.com`. The ClearTrust session will however be invalidated if the user logs out from the Portal.

Note:

If single sign-on is set to **on** but no display name or authentication order is configured for the ClearTrust authentication method on the VPN Gateway, it will not be possible to log in to the VPN without a valid CTSESSION cookie.

The default value is **off**.

20. In the **Domain Cookie Scope** field, enter the desired domain scope.

    This setting determines the value of the domain cookie when single sign-on is set to **on**.

    - Scope = `0`: The most specific domain name will be calculated from the host name. If the Portal's host name is `a.b.c.d.e`, the domain cookie's value will be `.b.c.d.e`.
    - Scope = `3`: If the Portal's host name is `a.b.c.d.e`, the domain cookie's value will be `.c.d.e`.
    - Scope = `2`: If the Portal's host name is `a.b.c.d.e`, the domain cookie's value will be `.d.e`.

    The scope must be either `0` or greater than or equal to `2`.

    The default value is `0`.

21. Click **Update**.

Configure ClearTrust Dispatchers

The Dispatcher is a ClearTrust component responsible for providing information to the RSA ClearTrust web server agents about the availability of the Authorization Servers. It enables the agents to choose a new authorization server at start-up or if a failure. See the ClearTrust documentation for more information about the Dispatcher component.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 113.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example **`cleartrust`**.
10. Enter the display name of the server.
11. Select **cleartrust** in **Mechanism** drop-down list.
12. Click Update.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Dispatchers** tab.
15. Click **Add**.

    The Add New Dispatcher form appears.
16. In the **Host Name** field, enter the host name of a ClearTrust dispatcher.

    This step lets you point out one or several Dispatchers that have previously been installed in the RSA ClearTrust setup.
17. In the **Authentication Port** field, enter the desired port number.

    If your ClearTrust dispatcher uses another port number you can change the default value of 5608.
18. Click **Update**.

Configure ClearTrust Authorization Servers

Instead of letting the dispatcher manage communication with the ClearTrust authorization server(s) you can have the web server agent (that is the AVG) communicate directly with the authorization server(s). Note that if a dispatcher is configured on the AVG, any authorization servers configured on the AVG will be ignored.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 114.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example cleartrust.
10. Enter the display name of the server.
11. Select **cleartrust** in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Authorization** tab.

    The Add New Server form appears.
15. In the **Host Name** field, enter the host name of a ClearTrust authorization server.
16. In the **Authentication Port** field, enter the desired port number.

    If your ClearTrust authorization server uses another port number you can change the default value of 5615.

    If needed, additional ClearTrust authorization servers can be added for redundancy.
17. Click **Update** and apply the changes.

Client Certificate Authentication

For instructions on how to configure client certificate authentication when using a ClearTrust authentications scheme, see.

Specify the Authentication Fallback Order

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.

4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.
7. Click on **Authentication Order** tab.

   The AuthOrder form appears.
8. Under **Fallback Order**, in the **Available** list, select **2 cleartrust**.
9. Click **>>** to move the item to the Selected list.

   To change the authentication order (if several authentication IDs have been configured), move all authentication IDs back to the Available list. Then move them back one at a time to the Selected list in the order that you wish authentication to be carried out.
10. Click **Update**.
11. Apply your changes.

    When a match of user name and password is found, the other specified authentication methods (if any) in the Authentication Order list are ignored.

RSA SecurID Authentication

The RSA SecurID authentication method lets you configure user authentication through an existing RSA SecurID server.

Add RSA Server(s)

These steps add one or more RSA servers that will be queried to perform user authentication.

1. In the System tree view, expand **Administration**.
2. Select **RSA Servers** and click **Add**.

   The Add New RSA Server form appears.
3. In the **RSA Server IP/Hostname** field, enter a symbolic name for the new RSA server.
4. Click **Update**.

   The RSA Servers form is redisplayed.
5. Select the check box next to the newly created RSA server's symbolic name and click **Edit**.

The Modify RSA Server form appears.

6. Under Import sdconf.rec file, next to the **File** field, click **Browse**.

   The folders in your file system are displayed. The sdconf.rec file is a configuration file that contains critical RSA ACE/Server information. Contact your RSA ACE/ Server administrator to obtain the file.

7. Find the sdconf.rec file and click **Open**.
8. Back in the Modify RSA Server form, click **Import**.

   The sdconf.rec file is imported to the VPN Gateway.

9. If required, add a new RSA server by repeating steps 1-8.

Configure Basic Settings

1. Logon as VPN Admin User.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server is displayed.

8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example rsa.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see Groups, Access Rules and Profiles on page 35.

10. In the **Display Name** field (optional), set the desired display name.

    The display name will appear in the Login Service list box on the Portal login page and in the SSL VPN client's login window. This is a way of directing the remote user to the proper authentication server, if the Portal uses different authentication methods.

    By selecting **default** in the Login Service list box on the Portal login page, authentication will be carried out according to the configured authentication order.

11. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.

    This step lets you specify an NTLM domain name that can be used in automatic login links (that is iauto, or Internal Auto Login URL), where the target backend server requires a Windows domain. The <*var:domain*> macro (if included in a link) expands to the domain name specified with this command.

    For more information about this link type, see Group Links on page 127.
12. Select **rsa** in **Mechanism** drop-down list.
13. Click **Update**.

Configure RSA SecurID Specific Settings

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 117.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example **`rsa`**.
10. Enter the display name of the server.
11. Select **rsa** in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Settings** tab.
15. In the Secondary Authentication Server field (optional), specify a second authentication server to be used after the first one succeeds.

    This feature is designed to support single-sign on to backend servers in cases where the first authentication method is token-based or uses client certificate authentication.

If a second authentication method is specified, an extra password field will be added to the Portal login page.

16. In the RSA Server IP/Hostname list box, select the RSA server symbolic name for the current authentication ID.

    This name identifies the RSA server and was configured in step 3 on page 115 in the section Add RSA Server(s) on page 115.

17. In the Group for RSA Authenticated Users list box, select the desired group name.

    This step sets the user access group (as defined on the VPN Gateway) to which authenticated users will be assigned. The access rules pertaining to this group will determine the user's access rights.

18. Click **Update**.
19. Apply the changes.

Specify the Authentication Fallback Order

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.
7. Click on **Authentication Order** tab.

   The AuthOrder form appears.

8. Under **Fallback Order**, in the **Available** list, select **2 rsa**.
9. Click **>>** to move the item to the Selected list.

   To change the authentication order (if several authentication IDs have been configured), move all authentication IDs back to the Available list. Then move them back one at a time to the Selected list in the order that you wish authentication to be carried out.

10. Click **Update**.
11. Apply your changes.

    When a match of user name and password is found, the other specified authentication methods (if any) in the Authentication Order list are ignored.

Local Database Authentication

The AVG device can act as an authentication database itself. It can store thousands of user authentication entries each defining a user name, password, and the relevant access groups. The local authentication method can be useful if no external authentication databases exist, for testing purposes or if speedy deployment is needed.

If you ran the VPN quick setup wizard during the initial setup procedure, local database authentication has already been created as authentication ID 1.

Configure Basic Settings

1. Logon as VPN Admin User.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server is displayed.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example local.

   A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see Groups, Access Rules and Profiles on page 35.
10. In the **Display Name** field (optional), set the desired display name.

    The display name will appear in the Login Service list box on the Portal login page and in the SSL VPN client's login window. This is a way of directing the remote user

to the proper authentication server, if the Portal uses different authentication methods.

By selecting **default** in the Login Service list box on the Portal login page, authentication will be carried out according to the configured authentication order.

11. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.

    This step lets you specify an NTLM domain name that can be used in automatic login links (that is iauto, or Internal Auto Login URL), where the target backend server requires a Windows domain. The <*var:domain*> macro (if included in a link) expands to the domain name specified with this command.

    For more information about this link type, see Group Links on page 127.

12. In the Group Authentication Servers list, you can specify that another authentication server should be used for retrieving group information (optional).

    Group information can only be retrieved from the Local database and LDAP databases. LDAP variables (if configured) are also retrieved. If user groups exist in the current authentication scheme, these will be added to the user groups found in the referenced authentication scheme(s).

    To be able to specify another server for group information retrieval, you have to configure this authentication server with an authentication ID of its own.

13. Click **Update**.

    Before you can start adding users to the local database, you should configure the authentication order (see the next section).

Specify the Authentication Fallback Order

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**.

7. Click on **Authentication Order** tab.

   The AuthOrder form appears.

8. Under **Fallback Order**, in the **Available** list, select **2 local**.
9. Click **>>** to move the item to the Selected list.

   To change the authentication order (if several authentication IDs have been configured), move all authentication IDs back to the Available list. Then move them back one at a time to the Selected list in the order that you wish authentication to be carried out.

   If you use Local Database for authentication in combination with other methods within the VPN, place the Local Database method first in the Authentication Order list, because it is performed extremely fast regardless of the number of users in the database.

10. Click **Update** and apply your changes.

    When a match of user name and password is found, the other specified authentication methods (if any) in the Authentication Order list are ignored.

Add Users to the Local Database

To be able to add a user to the local database, the group in which the user should be a member must have been configured on the VPN Gateway. For instructions on group configuration, see Groups, Access Rules and Profiles on page 35.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 122.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.

8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example **`local`**.
10. Enter the display name of the server.
11. Select local in **Mechanism** drop-down list.

12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Users** tab.

    The Users form appears.
15. Under **Users**, click **Add**.
16. Under **Add Single User**, in the **Name** field, enter the user's user name.

    To add bulk users under **Add Bulk Users**, see the section Add Bulk Users on page 122.
17. In the **Password** fields, enter the user's password.
18. Select the groups in which the user should be a member by moving them to the **Selected** list.
19. Click **Save User**.
20. To add a new user, repeat steps 3-7.

Add Bulk Users

A quicker way of adding users to the local database is to paste or enter a bulk of users (with passwords and groups) into the box under **Add Bulk Users**.

Enter the users on separate rows according to the following format:
john:password:group1,group2lisa:password:group1,group2,group3

Import User Database

The file you import must be in ASCII format and contain row entries with the required values separated by colon (:).

Example: username:password:group1,group2,group3

To be able to import a database file whose passwords were protected with a key when the file was exported, enter the same password key that was given at the time of export. To import a database file that is not protected with a key, enter any key (4 characters at a minimum) when prompted.

Existing entries in the local database will be overwritten by the imported database. Old databases with clear-text passwords can also be imported as well as databases with a mixture of encrypted and clear-text passwords. Clear-text passwords will be encrypted once the database is imported. Unencrypted passwords will be encrypted when upgrading from an older software version.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.

3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 123.

   Authentication Server screen appears.
7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example local.
10. Enter the display name of the server.
11. Select **local** in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Users** tab.

    The Users form appears.
15. In the Users form, click the **Import/Export** button.

    The Import/Export Local User Database from File form appears.
16. Under Import Local user Database from File, click **Browse**.

    The folders in your files system are displayed.
17. Find and select the file and click **Open**.

    The file name is displayed in the File field.
18. Click **Import**.

Export User Database

To export the existing user database to a file, proceed as follows:

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.

6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 124.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.

8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example local.
10. Enter the display name of the server.
11. Select **local** in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Users** tab.

    The Users form appears.

15. In the Users form, click the **Import/Export** button.

    The Import/Export Local User Database from File form appears.

16. Under **Export Local User Database to File**, in the **Secret key** field, enter the key used to protect user passwords.
17. Click **Export**.

    The user database file is retrieved from the VPN Gateway.

18. Save the file to disk.

List Registered Users

To list users added to the local database by user name and group membership, proceed as follows:

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.
5. Click on the VPN Gateway name for which authentication needs to be done.
6. Under settings, select **Authentication**. If Authentication server is already present go to 13 on page 125.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server form appears.
8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method, for example local.
10. Enter the display name of the server.
11. Select local in **Mechanism** drop-down list.
12. Click **Update**.
13. Click on the Authentication ID in Authentication Server screen.
14. Click on **Users** tab.

    The Users form appears.
15. To narrow your search, enter a string of characters directly followed by an asterisk (*) in the Prefix field.

    Example: By entering `je*` in the Prefix field, all entries with user names starting with `je` are displayed. To display all users, keep the asterisk in the Prefix field before proceeding.
16. In the **Max** list box, select the maximum number of users to display.
17. Click the **List** button.

    Registered users are displayed.

Chapter 8: Group Links

This chapter describes how to configure various types of hypertext links that appear on the Portal's Home tab.

Link Types

The following link types are available:

- SMB. Gives the user access to folders on an SMB (Windows file share) file server (Example 1: Link to SMB (Samba) File Server on page 130).
- FTP. Gives the useraccess to folders on an FTP file server (Example 2: Link to FTP File Server on page 132).
- External. Link (direct) to web page. Suitable for external web sites (Example 3: Direct Link to Web Page (External) on page 135).
- Internal. Link (secured) to web page. Suitable for internal web pages (Example 4: Secured Link to Web Page (Internal) on page 136).
- Iauto. Automatic login link (secured) to password-protected web page (Example 5: Automatic Login Link Secured by the AVG (Iauto) on page 138).
- Terminal. Link to terminal server through Java applet for Telnet or SSH connections (Example 6: Link to Terminal Server on page 142).
- HTTP Proxy. Link for accessing web pages through the AVG's HTTP Proxy server (Example 9: HTTP Proxy Link on page 160).
- FTP proxy. Application tunnel link to a specified FTP server (Example 10: FTP Proxy Link on page 163Example 10: FTP Proxy Link on page 163).
- Custom. Application tunnel link to a specified application server (Example 7a: Custom Port Forwarder Link on page 144).
- Telnet. Application tunnel link to terminal server for Telnet connections Example 6: Link to Terminal Server on page 142.
- Mail. Application tunnel link to mail server Example: Access to Outlook Express on page 299.
- Netdrive. Application tunnel link for mapping a network drive to an SMB (Windows file share) file server Create a Linkset for File Server Access on page 129.
- WTS. Application tunnel link to Windows Terminal Server Example 7b: Windows Terminal Server Port Forwarder Link with Automatic Portal Login on page 149.
- Citrix. Application tunnel link to Citrix server Example 5a: Automatic Login Link to Citrix Metaframe Server on page 140.

- Outlook. Application tunnel link to Microsoft Exchange server (Example 8: Outlook Port Forwarder Link on page 155).
- Net Direct. Portal link used to download and start the Net Direct client (downloadable version of the SSL VPN client (Server Configuration on page 173).
- Virtual Desktop. Virtual desktop link is used to configure Virtual Desktop settings for the current VPN Virtual Desktop on page 167.

Linksets

Each user group can be provided with one or several linksets. The linkset itself contains one or several links. The linksets and included links appear on the Portal's **Home** tab for the user to access intranet or Internet web sites, mail servers, file servers or web applications. When a group member is logged in, all linksets mapped to the user's group will be displayed.

The purpose of creating linksets is that once the linkset is created, it can be mapped to several user groups. Thus, links that should be common to several user groups can easily be assigned to the desired groups, without the need to create the links over and over again for each group. For group-specific links, simply create a linkset that is exclusive for that group.

Make sure that access to the resource provided through the link is not contradicted by any access rules that apply to the group(s) in which the remote user is a member.

Linkset Name

The linkset name (set with the **`name`** command) is used to map the linkset to the desired user access group.

Linkset Text

Optionally, using the **`text`** command, the linkset can be provided with a heading that is displayed on the Portal's Home tab. Using HTML tags, the heading can be formatted as desired.

Autorun Support

With autorun support enabled, all links in the linkset will be executed automatically as soon as the remote user is logged in to the Portal. The links will not be visible on the Portal's Home tab.

Configuration Examples

This section includes examples of how to create linksets with different link types and shows how to map the linksets to groups.

Create a Linkset for File Server Access

In this example we will create a specific linkset for file server access. The linkset should include two links, one for access to an SMB (Windows file share) file server and one for access to an FTP server.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. Click **Add**.

   The Add New Linkset form appears.

5. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

6. In the Text field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example Heading for a boldface heading.

   In the following example, the FONT tag (<FONT FACE="Impact">File server access</FONT>) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

7. Click **Update**.

8. Apply the changes.

Example 1: Link to SMB (Samba) File Server

As one of the links in the linkset we have just created, create a direct link to the home share folder of the currently logged on user. This link type should be used for SMB (Windows file share) file servers.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

   The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to be displayed on the Portal's Home tab.

In this example, enter the text `Link to home share folder`.

13. In the **Link Type** list box, select the desired link type, that is SMB.
14. Click **Continue**.

    The form is expanded.
15. Under **SMB Link Settings**, in the **Host** field, enter the file server host.

    The file server host can be entered as an IP address or a host name.
16. In the **Windows Domain/Workgroup** field (optional), enter the name of the desired Windows domain or workgroup.
17. In the **Share** field (optional), enter the name of a shared network folder.

    In this example we will create a link to the currently logged in user's home share folder. This can be achieved by including the <var:user> macro. The macro expands to the remote user's user name as provided on the Portal login page.

    Example: `home share/ <var:user>`

    To provide access to a folder on a lower level in the file structure, simply add a forward slash (/) and the folder name, for example `home share/ <var:user> / manuals/drafts`. Folder names are not case sensitive and spaces can be used in folder names.

    Note:

    When configuring an SMB (Windows file share) link to be displayed on a PDA Portal, specifying a shared network folder is required.
18. To add the host to the system's list of single sign-on domains, check the **Add Host to SSO Domains** check box (optional).

    For security reasons, automatic login to the SMB file server (using the Portal login credentials) is only possible if the SMB server's domain name or IP address is specified as a single sign-on domain, here or under **VPN Gateways>Gateway Setup>Single Sign-On>Domains**.

    If not, an error message will be displayed to the user, saying that single sign-on is not allowed. The folder specified in the link will however be shown when the user enters his password in the **Password** field and clicks the **Open** button on the Portal's **Files** tab.

    Single sign-on is however always possible if the user name and password is specified in the link. Enter the link specification in the **Host** field, for example: `user:password@smb.example.com`.
19. Click **Update**.
20. Apply the changes.

Example 2: Link to FTP File Server

This example shows how to create a direct link to an FTP file server.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.

5. Click **Add**.

   The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.

9. Apply the changes.

10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    Add Portal Links form appears.

12. In the **Text** field, enter the clickable text to appear on the Portal's Home tab.

    In this example, enter the text `Link to FTP file server`.

13. In the **Link Type** list box, select **FTP**.

14. Click **Continue**.

    The form is expanded.

15. In the **Server** field, enter the file server host.

    The file server host can be entered as an IP address or a host name.

16. In the **Initial Path on Host** field, enter the path to the desired directory.

    By specifying an initial path, a specific directory can be listed right away when the user clicks the link. In this example, the initial path /! is specified. For FTP servers, this translates into the currently logged in user's home directory.

    Like with the SMB link, macros can be used. To provide access to a folder or file on a lower level in the file structure, the initial path syntax could be as follows: `/home/share/<var:user>/Manuals/drafts/`. Note that directory names are case sensitive for FTP file servers. Spaces can however be used in directory names.

17. To add the file server to the system's list of single sign-on domains, check the **Add Server to SSO Domains** check box (optional).

    Note:

    For security reasons, automatic login to the FTP file server (using the Portal login credentials) is only possible if the file server's domain name or IP address is specified as a single sign-on domain, here or under **VPN Gateways>Gateway Setup>Single Sign-On>Domains**.

    If not, an error message will be displayed to the user saying that single sign-on is not allowed. The directory specified in the link will however be shown after the user has entered his password in the **Password** field and clicked the **Open** button on the Portal's **Files** tab.

    Single sign-on is however always possible if the user name and password is specified in the link. Enter the link specification in the **Server** field, for example: **`user:password@ftp.example.com`**. For anonymous mode, enter **`ftp`** or **`anonymous`** before the colon (:) and any text string after the colon.

18. Click **Update** and apply the changes.

View Created Links in BBI

1. To view the new links, select **VPN Gateways** in system tree view.
2. Under **Settings**, click on **Linksets**.

   The links we have just created are displayed in the order they will be displayed on the Portal's Home tab.

3. To move a link up or down in the list, click the arrows in the **Reorder** column.
4. Apply the changes.

Map the Linkset to a Group

1. In the system tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
2. Click on the VPN Gateway name.

   VPN Summary screen appears.
3. Under **Settings**, click on **Groups**.

   Groups form appears.

4. In the **Group** list box, select the group to which the linkset should be mapped.

   In this example, the linkset we created on Create a Linkset for File Server Access on page 129, that is files, should be mapped to the staff group. This step assumes that we have previously created a group called staff.
5. Click **Refresh**.

   Modify a Group form appears.
6. In the **Portal Linksets** list box, select the linkset you wish to map to the group, that is **files**.
7. Click **Add**.
8. Apply the changes.

   When a member of the staff group logs in to the Portal, Linkset 1 (including the two file server links) will be visible on the **Home** tab.

Other Link Types

The following sections provide examples on how to configure the other available link types. The instructions assume that you are familiar with creating linksets and mapping linksets to groups. If not, read the previous section, Create a Linkset for File Server Access on page 129.

Example 3: Direct Link to Web Page (External)

This example shows how to create a link to a web page. As opposed to the internal link, the external link directs the HTTP request straight to the specified resource, that is without adding the AVG rewrite prefix (compare to Example 4: Secured Link to Web Page (Internal) on page 136).

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

   The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.

10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the link text `Link to Avaya's public web site`.

13. In the **Link Type** list box, select the desired link type, that is **External Website**.
14. Click **Continue**.

    The form is expanded.

15. Under **External Link Settings**, in the **Protocol** list box, select the desired access protocol, that is **http** or **https**.
16. In the **Host** field, enter the address (FQDN) of the web site to which the link should direct the user.
17. In the **Path** field, enter the path on the web server.

    A path must always be specified. When a forward slash (`/`) is specified as the path, the document root of the web server is implied.

18. Click **Update**.
19. Apply the changes.

Example 4: Secured Link to Web Page (Internal)

This example shows how to create a secure link to an internal web page on your intranet. The internal link directs the HTTP request to the VPN Gateway, where the rewrite prefix (boldface) is added to the link.

Example: `https://vip.example.com/http/inside.example.com/`

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the link text `Link to internal phone list`.

13. In the **Link Type** list box, select the desired link type, that is **Internal Website**.
14. Click **Continue**.

    The form is expanded.

15. Under **Internal Link Settings**, in the **Protocol** list box, select the desired access protocol, that is **http** or **https**.
16. In the **Host** field, enter the address (FQDN) of the web site to which the link should direct the user.
17. In the **Path** field, enter the path on the web server.

    A path must always be specified. When a forward slash (`/`) is specified as the path, the document root of the web server is implied.

    To create a link to the currently logged in user's home page (if any) on the intranet, you can use the <var:user> macro as an element in the specified path: Example: `/~<var:user>`.

18. Click **Update**.
19. Apply the changes.

Example 5: Automatic Login Link Secured by the AVG (Iauto)

This example shows how to create an automatic login link to a password-protected web page. The HTTP request is directed to the AVG, where the rewrite prefix (boldface) is added to the link.

Example: `https://vip.example.com/https/inside.example.com/`

The Internal Auto Login URL (iauto) link supports form-based authentication as well as HTTP-based authentication, such as NTLM or basic (www-authenticate). The AVG automatically retrieves the URL to analyze which type of authentication method it uses.

For an example on how to use the iauto link together with a port forwarder, see Example 7c: Windows Terminal Server Port Forwarder Link with Automatic Backend Server Login on page 151.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
2. Click on the VPN Gateway name.

   VPN Summary screen appears.
3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.
4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

   The Add New Linkset form appears.
6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.
7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.
11. Click **Add**.

    The Add Portal Links form appears.
12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.
13. Define the link text to appear on the Portal's Home tab.

    In this example we will enter the link text `Secure auto-logon link to web page`.
14. In the **Link Type** list box, select the desired link type, that is **Internal Auto Login URL**.
15. Click **Continue**.

    The form is expanded.
16. Under Iauto Link Settings, in the Login URL field, enter the URL to the password-protected web page.

    Example 1 (HTTP-based authentication): `http://inside.example.com/login/login.htm`

    Example 2 (form-based authentication): `http://inside.example.com/login/login.asp`
17. Click **Submit**.

    The AVG automatically retrieves the URL to analyze which authentication type it uses.

    Example 1: In this example, a web page using HTTP-based authentication was found. The following message is displayed in the BBI:

    A link to the web page has been created. When the user clicks the link on the Portal's Home tab, the AVG automatically attempts to authenticate to the web page using the credentials provided by the user on Portal login. If successful, the user is automatically logged in. If not, the AVG generates a temporary form for the user to log in with the required credentials.

    If the web server requires a domain name along with user name, change the **Mode** setting (under **VPN Gateways>Portal Linksets>Links>Iauto>Auto Configuration**) from normal to add_domain.

Example 2. In this example, a web page using form-based authentication was found. The input fields found on the form are displayed in the BBI for you to specify what values to insert in the fields when the user clicks the **iauto** link.

In the preceding example, the **user** and **password** fields were found on the form. The names correspond to the input name value in the web page's source code.

Enter the values to be inserted in the fields. Macros, text strings or a combination of both can be used. By using the <var:user> and <var:password> macros as values (as in the preceding example), the macros will expand to the credentials provided by the remote user on the Portal login page. If these are the credentials that the target web page requires, the user is automatically logged in. If not, the web page's form appears instead.

The <var:domain> macro can be used if the form includes an input field for a Windows domain. In this case, the macro will expand to the domain name specified in the **Domain Name** field for the current authentication ID (under **VPN Gateways>Authentication>(Method)>General**).

18. Click **Submit**.

    If needed, the values that you have specified can later be edited under Internal Auto Mapping (**VPN Gateways>Portal Linksets>Links>Iauto>Auto Configuration**).

    This is also where link properties like authentication type (auto, get, post or web), method (http or https), host, path, mode (normal or add domain) and cookies can be edited separately.

    For a full account of available **`iauto`** commands, see the *Avaya Command Reference*.

19. Apply the changes.

Example 5a: Automatic Login Link to Citrix Metaframe Server

This example shows how to configure a single sign-on link to Web Interface 2.0 and Web Interface 3.0 on a Citrix Metaframe server.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the link text `Single sign-on to Citrix Metaframe Server`.

13. In the **Link Type** list box, select the desired link type, that is **Internal Auto Login URL**.
14. Click **Continue**.

    The form is expanded.

15. In the **Login URL** field, enter the URL to the password-protected web page.

    Example 1 (Web Interface 2.0):

    ```
    http://citrix.example.com/Citrix/MetaFrameXP/default/
    login.asp?ClientDetection=On
    ```

    Example 2 (Web Interface 3.0):

    ```
    http://citrix.example.com/Citrix/MetaFrame/default/
    login.aspx?ClientDetection=On
    ```

16. Click **Submit**.

The AVG automatically retrieves the URL to analyze which authentication type it uses.

In the preceding example, the **user**, **password** and **domain** fields were found on the form and need to be completed with the desired values.

Enter the values to be inserted in the fields. Macros, text strings or a combination of both can be used. By using the <var:user> and <var:password> macros as values (as in the preceding example), the macros will expand to the credentials provided by the remote user on the Portal login page. If these are the credentials that the target web page requires, the user is automatically logged in. If not, the web page's form appears instead.

The <var:domain> macro can be used if the form includes an input field for a Windows domain. In this case, the macro will expand to the domain name specified in the **Domain Name** field for the current authentication ID (under **VPN Gateways>Authentication>(Method)>General**).

17. Click **Submit**.

    If needed, the values that you have specified can later be edited under Internal Auto Mapping (**VPN Gateways>Portal Linksets>Links>Iauto>Auto Configuration**).

    This is also where link properties like authentication type (auto, get, post or web), method (http or https), host, path, mode (normal or add domain) and cookies can be edited separately.

    For a full account of available **`iauto`** commands, see the *Command Reference*.

18. Apply the changes.

Example 6: Link to Terminal Server

This example shows how to create a link to a terminal server using Telnet or SSH. When the remote user clicks the link, a terminal window is opened in a new browser window by way of a Telnet/SSH terminal Java applet.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the link text `Terminal access`.

13. In the **Link Type** list box, select the desired link type, that is **Terminal**.
14. Click **Continue**.
15. Under **Terminal Link Settings**, in the Remote Host field, enter the IP address or host name of the remote terminal server, for example `terminal.example.com.`
16. In the **Remote Port** list box, select the remote port.

    TCP port 23 is the default port used for Telnet. If you want to use SSH, specify TCP port 22 as the remote port.

17. In the **Remote Protocol** list box, select the desired terminal access protocol, that is **telnet, ssh** or **sshv2**.

    To enable display of applications with graphical user interfaces, SSH version 2 (sshv2) supports X11 forwarding.

18. In the **Keymap URL** field (optional), enter the path to a keyboard mapping file.

    If a keymap URL is specified, the user's keyboard mappings can be configured through an external configuration file located on the specified web server.

This feature is designed for users with non-standard keyboards. Example: When prompted for a keymap URL, enter the URL, path (if any) and finally the name of the keyboard mapping file, for example `http://inside.example.com/keyCodes.at386`.

Documentation describing the configuration file properties in Appendix F, "Definition of Key Codes " in the *User's Guide.*

19. To display the HTTP Proxy Host Settings form, click the **HTTP Proxy Host Settings** link (shown top right in the form above) or scroll down.
20. In the **HTTP Proxy Host** and **Port** fields (optional), enter the address and port of an intermediate HTTP Proxy server (if any).

    If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

    Skipping the prompts means that all applet traffic will be tunneled directly to the AVG, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.
21. If an intermediate HTTP Proxy server is specified, enter the credentials required to access this server (if needed) in the HTTP Proxy Username and Password fields.
22. Click **Update** and apply the changes.

    When the remote user clicks the Telnet or SSH link on the Portal, a terminal window opens (in the SSH case, the user has to log in first). To be able to type anything in the terminal window, the user must first click on the window (anywhere) to activate it.

Example 7a: Custom Port Forwarder Link

By clicking a Port Forwarder link, the remote user is provided with one or more secure tunnels to an intranet application server. The purpose is to be able to run one or more UDP- or TCP-based client applications, for example Telnet or Windows Terminal Server, towards a specified application server.

When the user clicks the link, a Java applet is downloaded. The Java applet is instructed to listen to a port number on the user's own computer (that is 127.0.0.1 or any other IP address within the 127.x.y.z range). The applet then forwards all incoming traffic to an application server on the intranet.

Setting up a Port Forwarder link to be displayed on the Portal's Home tab (instead of letting the user set up a Port Forwarder on the Portal's Advanced tab) is a way of making application access simpler for the user. In addition, group members whose user type is set to novice or

medium will not have access to the **Advanced** tab. A third advantage with the Port Forwarder link is that it can be set to launch the application automatically.

Using the Port Forwarder API (see page Port Forwarder API on page 159), you can develop a custom application that automatically logs in the user to the VPN and executes the Port Forwarder link.

Note:

The Custom Port Forwarding link type (exemplified here) lets you configure a port forwarder link for an application of your own choice. Examples 7a, 7b and 7c show ways of applying the custom port forwarder for two different applications, Telnet and Windows Terminal Server. Another way of configuring port forwarder links for these applications is to use the Telnet Port Forwarding and Windows Terminal Server link types. The only difference is that some relevant parameters (like port numbers) are suggested automatically by the wizards. Other available port forwarder link types are Netdrive Port Forwarding, Mail Port Forwarding and Outlook Port Forwarding.

The following example describes how to set up a custom port forwarder link to a Telnet server.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.

5. Click **Add**.

   The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.
11. Click **Add**.

    The Add Portal Links form appears.
12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the link text `Link to Telnet server`.
13. In the **Link Type** list box, select the desired link type, that is **Custom Port Forwarding**.
14. Click **Continue**.
15. In the System tree view, under Custom Forwarder, select **Tunnel**.

    The Tunnel form appears.
16. Click **Add**.

    The Custom Links form appears.
17. In the **Traffic Mode** list box, select the desired traffic mode for the current tunnel.
18. In the **Local IP** field, enter the local host IP address (or keep the default value).

    The SSL tunnel will be established between the specified TCP/UDP port on the user's local machine (local host IP=any IP address within the 127.x.y.z range) and the VPN Gateway.
19. In the **Local Port** field, enter the local port (or keep the default value).

    When specifying the local port, use port numbers just above 5000 which are usually free to use or use the application-specific port number. On Windows machines any port number can be used.
20. In the **Remote Destination Host** field, enter the destination host (IP address or host name).

    The VPN Gateway relays data from the user's local machine to the specified target (destination host) and application-specific port (destination port).

    In this example we will specify `telnet.example.com` as host.
21. In the **Remote Destination Port** field, enter the destination port.

    The destination port number we will use in this example is 23, which is the well-known port number for Telnet connections.
22. In the **Host Mapping** field, enter the desired host mapping (optional).

    Host mapping can be specified for example if the user should start the application manually. Example: If the host alias is telnet and the local port number 5004, the

user can start the Telnet client and use `telnet 5004` as host name/port to connect to the server specified as destination host.

Note:

Usage of host aliases requires the alias to be mentioned in the Java applet window (see 28 on page 148). It also requires the user to have administrator privileges on the client computer or have write access enabled for the hosts and lmhosts files. Hosts and lmhosts files are located in `%windir%\hosts` on Windows 98 and ME and in `%windir%\system32\drivers\etc\hosts` on NT, XP and Windows 2000.

23. Click **Update**.

    The tunnel is added to the Tunnel form.

24. To create another tunnel (if required), click **Add**.

    In this example, one connection is sufficient for the link we are configuring. However, one single Port forwarder link can be configured to set up multiple tunnel connections. For example, to configure an Outlook Express link, you have to configure the Port forwarder link to set up one connection to an SMTP server and another to a POP3 server.

25. In the System tree view, under Custom Forwarder, select **General**.

26. Under **Port Forwarder Link Settings**, in the Executable Name field, specify the application to be started (optional).

    This step defines the application to be started when the user clicks the link, for example **`cmd.exe`** to open the Command window. If the field is left blank, no application will be started when the user clicks the link. The user can however be instructed to start the application manually (see 28 on page 148). If **`browser`** is entered as executable, the user's default browser will be started.

    Note:

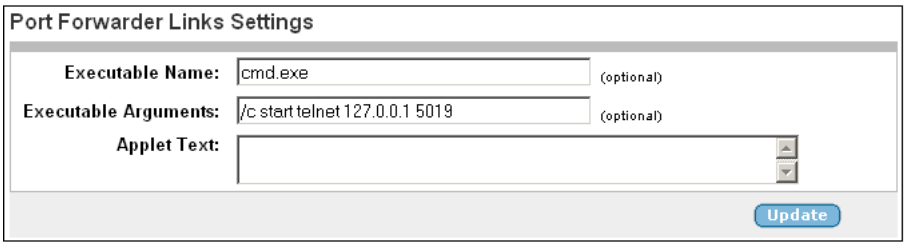
    The VPN Gateway must be able to find the executable either through the PATH variable or in the registry (on Windows clients), that is `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths`. To make sure the program is found, the complete path to the executable can also be entered in the **Executable Name** field.

    Generally, only graphical applications (that is applications that open their own windows) can be started using the Port forwarder link. This example describes how to open the Command window (cmd.exe) to run the Telnet client.

27. In the Executable Arguments field, specify an argument to the application (optional).

The argument identifies the command-line argument to be used by the application, for example `http://127.0.0.1:5004` if the executable is browser. Note that each application has its own set of arguments.

In the following example, the executable is entered without a path. The argument to cmd.exe tells the application to start Telnet and connect to the local host IP address and port we specified in 18 on page 146.



28. In the **Applet Text** field, enter a custom text (for example with user instructions) to be displayed in the Java applet window (optional).

    The custom text (if entered or pasted) will be displayed in the Java applet window automatically displayed when the user clicks the link. The instructions can for example be used to explain the purpose of the port forwarder(s) or how to launch the application (for example by using the specified host alias).

    If no custom text is entered, a standard text is displayed in the **Info** part of the Java applet window. Following is an example of a Java applet standard text:

```
This is a port forwarder. It securely forwards network traffic
into your corporate network.
If you close this window the port forwarder will be stopped.
This window will be minimized as soon as the port forwarder is
ready.
```

29. Click **Update**.
30. In the System tree view, under **Custom Forwarder**, select **HTTP Proxy**.

    The HTTP Proxy Host Settings form appears.

31. In the **HTTP Proxy Host** and **Port** fields (optional), enter the address and port of an intermediate HTTP Proxy server (if any).

    If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or domain name) and port

of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Skipping the fields means that all applet traffic will be tunneled directly to the AVG, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.

32. If an intermediate HTTP Proxy server is specified, enter the credentials required to access this server (if needed) in the HTTP Proxy Username and Password fields.
33. Click **Update**.
34. Apply the changes.

    When the remote user clicks the custom port forwarder link we have created in this example, the Command window is started. A command used to open Telnet and connect to the specified Telnet server is automatically executed.

Example 7b: Windows Terminal Server Port Forwarder Link with Automatic Portal Login

This example describes a more advanced application of the Port Forwarder link. It shows how the <var:portal> macro can be included in the argument to have the browser connect to a terminal applet residing on an intranet web host used for Windows Terminal Server sessions. The terminal applet in its turn will be instructed to connect to the user's local machine to enable a secure SSL session.

Note:

Instead of creating a custom port forwarder link to a Windows Terminal Server, we recommend using the Windows Terminal Server link type. It automatically provides the relevant port numbers for the link in a wizard. This example just uses the WTS application to show the principles of configuring a custom port forwarder link.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
2. Click on the VPN Gateway name.

   VPN Summary screen appears.
3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.
4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

   The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the link text `Link to Windows Terminal Server`.

13. In the **Link Type** list box, select the desired link type, that is **Custom Port Forwarding**.
14. Click **Continue**.
15. In the System tree view, under Custom Forwarder, select **Tunnel**.

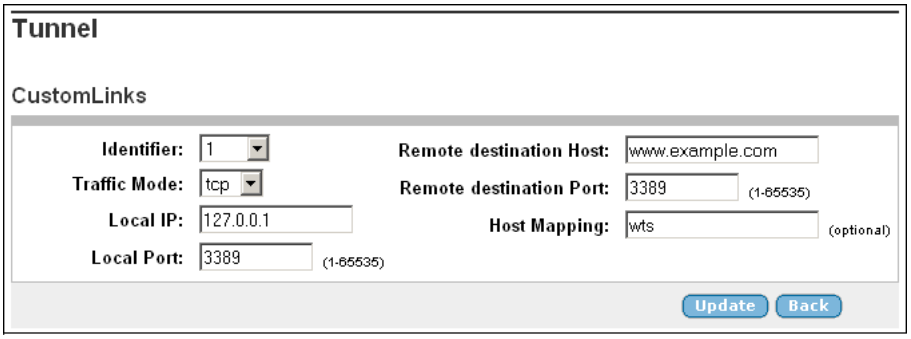
    The Tunnel form appears.

16. Click **Add**.

    The Custom Links form appears.

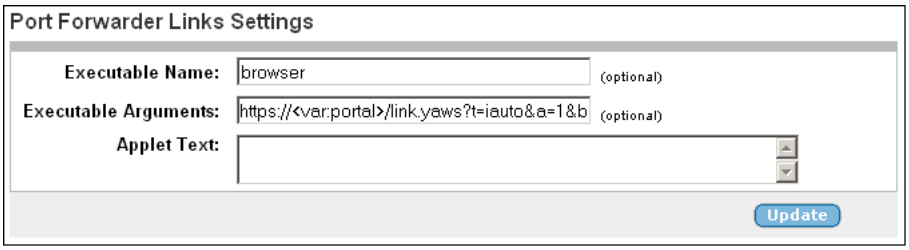
17. Enter the tunnel specifics.

    In this example, a terminal applet on the Windows Terminal Server web page should be instructed to connect to source IP address 127.0.0.1 on port 3389, which is the application-specific port number for Windows Terminal Server sessions.



18. Click **Update**.
19. In the System tree view, under Custom Forwarder, select **General**.
20. Under **Port Forwarder Links Settings**, enter the application specifics.

    When the user clicks the link, a new browser window opens. For the browser to be able to access the terminal applet on the intranet host, the connection has to be made through the Portal. This is done by including the <var:portal> macro in the argument. The macro expands to the Portal's IP address.



    The full argument in the Executable Arguments field reads: `https://<var:portal>/http/www.example.com/TSWeb/connect_new_server.asp?Server=127.0.0.1`

21. Click **Update**.

    For more detailed descriptions of each field, see example 7a on Example 7a: Custom Port Forwarder Link on page 144.

22. Apply the changes.

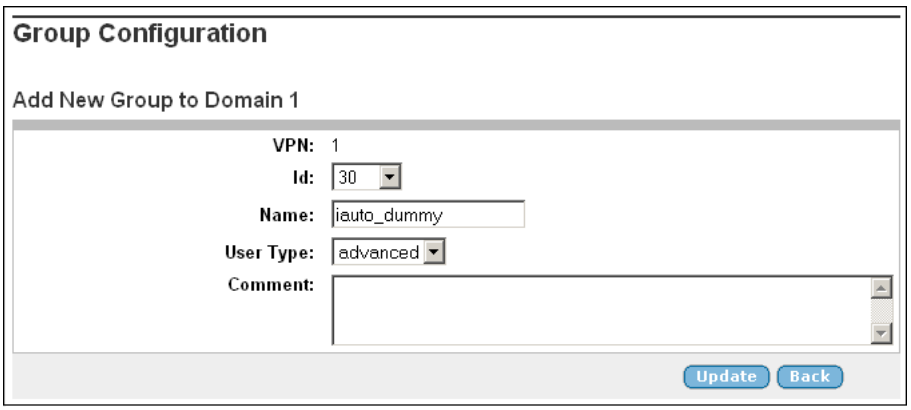
Example 7c: Windows Terminal Server Port Forwarder Link with Automatic Backend Server Login

This example describes an even more advanced scenario – almost identical to the one described in example 7b – but here the backend server requires user authentication. To enable the remote user to access the resource with one single click, the Port Forwarder and Internal Auto Login URL (iauto) links will have to be combined.

1. In the system tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.
3. Under **Settings**, select **Groups**.
4. Click **Add** and create a dummy group.

   The purpose of creating a dummy group is to hide the iauto link. We will later embed the iauto link in the port forwarder link. Because no user belongs to the dummy group, the iauto link will not be visible.

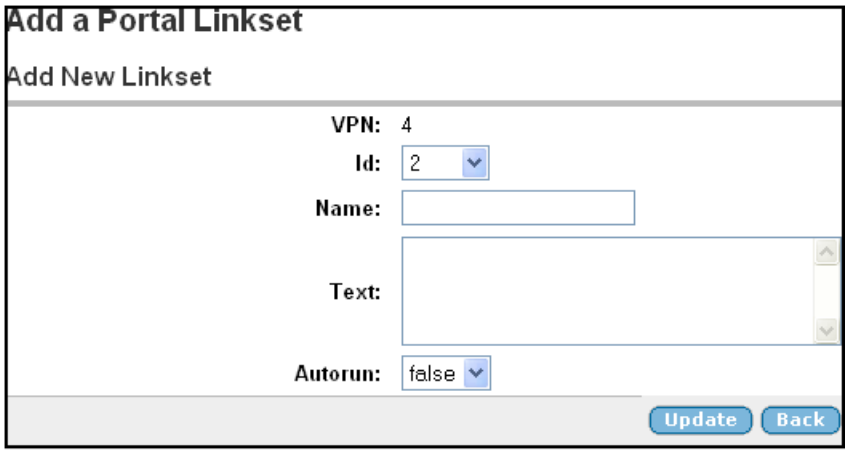
   Configure the dummy group as number 30.



5. Click **Update**.
6. In the system tree view, select **VPN Gateways**.
7. Select the name of the VPN Gateway.
8. Under **Settings**, select **Link Sets**.

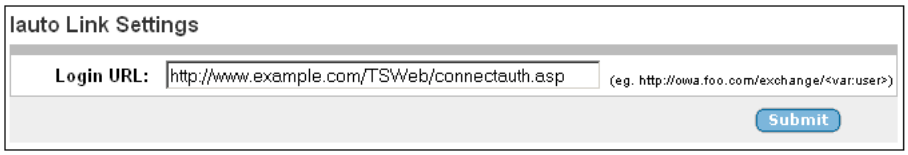
   The Portal Linksets form appears.
9. Click **Add**.

   The Add New Linkset form appears.
10. Enter the following information for the new linkset.



11. Click **Update**.
12. Click on the name of the portal linkset.
13. Click on **Portal Links** tab and then click on **Add**.
14. In the **Text** field, enter the link text `iauto for port forwarder`.
15. In the **Link Type** list box, select **Internal Auto Login URL** as link type.
16. Click **Continue**.

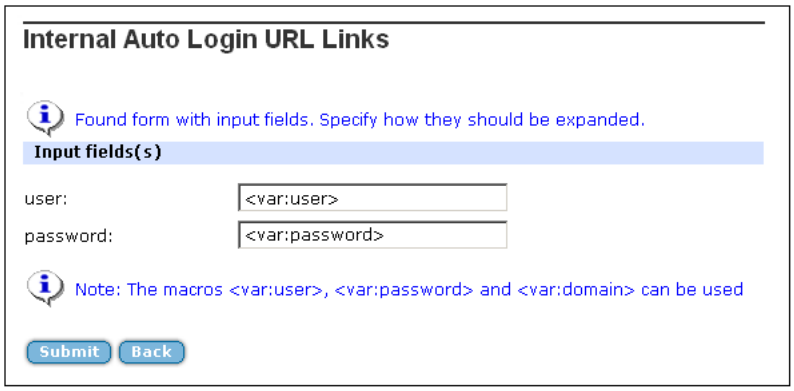
    The form is expanded.
17. In the **Login URL** field, enter the URL for authenticating to the Windows Terminal Server.



18. Click **Submit**.

    The system retrieves the page to analyze the type of authentication used.

    The input fields found on the form are displayed in the BBI for you to specify what values to insert in the fields when the user clicks the **iauto** link.
19. Enter values for the input fields found on the form.



20. Click **Submit**.
21. In system tree view, select **VPN Gateways**.
22. Select the name of the VPN.
23. Under **Settings**, select **Groups**.
24. In the **Group** list box, select the group to which the portal linkset should be mapped.

    Select the dummy group we created in 4 on page 152.
25. Click on **Linksets** tab.
26. In the **Portal Linksets** list box, select **iauto** (the linkset we created in 8 on page 152).
27. Click **Add**.
28. In the system tree view, select **VPN Gateways**.

    The following steps describe how to configure the port forwarder link where the iauto link should be embedded.
29. Select the name of the VPN Gateway.
30. Under **Settings**, select **Linksets**.
31. Select the name of the portal linkset and click on **Portal Link** tab.
32. Click **Add**.

    The Add Portal Links form appears.
33. In the **Text** field, enter the link text to be displayed on the Portal's Home tab.

    Enter the link text `WTS auto-login link`.
34. In the **Link Type** list box, select **Custom Port Forwarding**.
35. Click **Continue**.

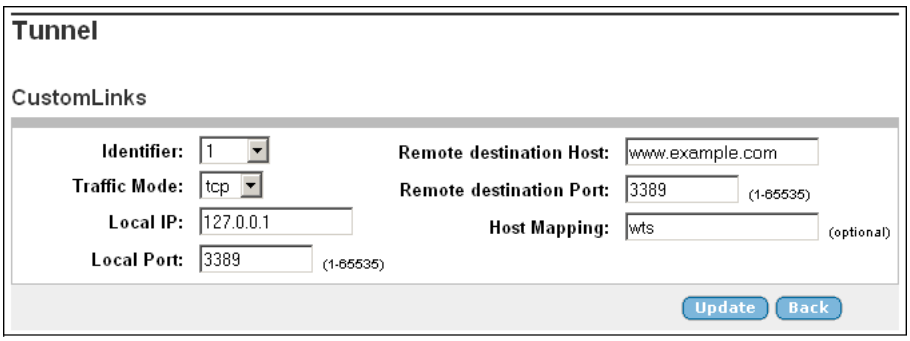
    Portal Links from in displayed.
36. Click on **Tunnel** tab.

37. Click **Add**.

    The Tunnel form appears.

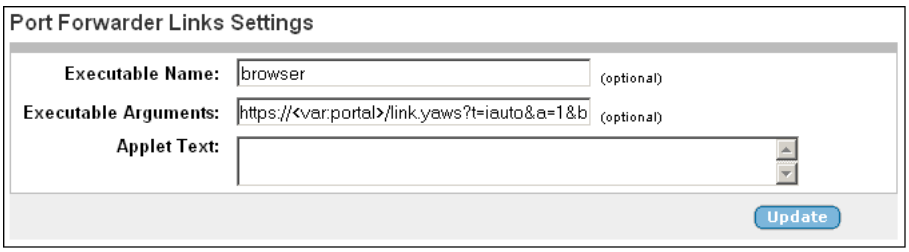
38. Enter the tunnel specifics.

    This example uses the same tunnel settings as example 7b.



39. Click **Update**.
40. In portal Link form, click on **General** tab.
41. Enter the application specifics.

    The only difference compared to example 7b, is that the iauto link we created initially is included in the executable argument instead of the web server address.



    The full argument in the Executable Arguments field reads:

    `https://<var:portal>/link.yaws?t=iauto&a=1&b=2&c=1`

    The argument includes the string "`link.yaws?t=iauto&a=1&b=2&c=1`" where a = xnet id (1), b = linkset id (2), c = link id (1). Xnet ID is equivalent to VPN ID.

    The *<var:portal>* macro is still present because the connection to the intranet web server is made through the Portal. The macro expands to the Portal's IP address.

42. Click **Update** and apply the changes.

Example 8: Outlook Port Forwarder Link

This example shows how to create a Port forwarder link to a Microsoft Exchange server on the intranet, enabling secure transfer of mail messages, calendar, address book entries and similar.

For the Outlook Port forwarder to work, the following prerequisites must be fulfilled:

- The Exchange server's domain name suffix must be configured in the **Search List** field (under **VPN Gateways>Gateway Setup>DNS**). See 26 on page 159.
- The user must have administrator's rights on his/her computer or have write access enabled for the hosts and lmhosts files. Hosts and lmhosts files are located in `%windir%\hosts` on Windows 98 and ME and in `%windir%\system32\drivers\etc\hosts` on NT, XP and Windows 2000.
- The user's client machine must be of the **Hybrid** or **Unknown** node type. The node type can be checked by entering `ipconfig /all` at the DOS prompt.

  To change the node type to Hybrid (if needed), go to the registry editor folder `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`. If not already present, add a new DWORD Value called NodeType. Double-click NodeType and enter 8 in the Value Data field. Click OK and restart the computer.
- The Outlook Port forwarder link is meant to be used by clients connecting to the VPN Gateway from outside the intranet. If the client has direct connectivity to the intranet, the Port forwarder will fail. If the client has access to intranet DNS servers, communication will fail as well.
- To test DNS resolution, the VPN Gateway should be able to ping the Exchange server from the CLI, using the fully qualified name (FQDN).
- The user's Outlook account must be hosted on the Exchange server(s) specified in the Port forwarder.
- The Outlook Port forwarder link will not work if a proxy server is configured in the client browser. This also means that a HTTP Proxy link or HTTP Proxy portal session cannot be active at the same time as the Outlook Port forwarder.
- If you expect the connection to include more than 15 minutes of inactivity, increase the Client TCP Keep Alive Timeout value (under **VPN Gateways>Gateway Setup>SSL>TCP**).
- To ensure proper operation, specify the DNS name of the portal server in the **DNS Name of VIP field** (under **VPN Gateways>Gateway Setup>SSL>General**.
- If a firewall exists between the VPN Gateway and the Exchange server, the firewall settings must allow traffic to the required Exchange server ports. Note that these may vary with your environment. More information can be found on http://support.microsoft.com, for example Knowledge Base Articles 280132, 270836, 155831, 176466, 148732, 155831, 298369, 194952, 256976, 302914, 180795 and 176466.
- When a user clicks an embedded link in an e-mail message, the web site associated with the link must be displayed in a new instance of Internet Explorer. In Internet Explorer, go to the **Tools** menu and select **Internet Options**. Under the **Advanced** tab, go to **Browsing** and deselect the **Reuse windows for launching shortcuts** option.

This is how to create an Outlook port forwarder link to be displayed on the Portal:

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.

5. Click **Add**.

   The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.

9. Apply the changes.

10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the text `Link to Outlook`.

13. In the **Link Type** list box, select the desired link type, that is **Outlook Port Forwarding**.

14. Click **Continue**.

15. In the System tree view, under Outlook Forwarder, select **Tunnel**.

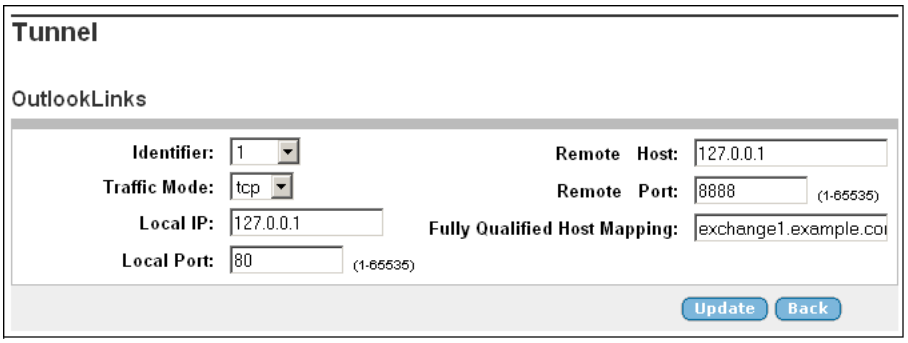
    The Tunnel form appears.

16. Click **Add**.

    The Outlook Links form appears.

17. Enter the tunnel specifics.

    The local host IP address should be set to 127.0.0.1 or any other IP address in the 127.x.y.z range. The Exchange server address must be entered as a fully qualified domain name (FQDN) and not as an IP address.



    The host entered in the Fully Qualified Host Mapping field reads `exchange1.example.com`.

18. Click **Update**.

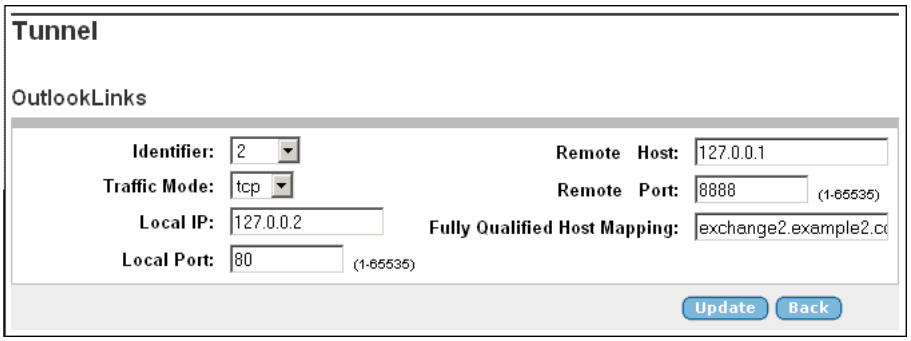
    The Tunnel form is redisplayed.

19. Click **Add** to create another port forwarder (if required).

    The services provided by the Exchange server (mail, calendar, address book and so on) may be distributed between different Exchange servers. If this is the case, you have the option to create several tunnels where the relevant Exchange servers can be specified.

20. Enter the tunnel specifics.

    If several tunnels are required, note that each tunnel must have a unique source IP address. A new source IP address is automatically suggested by the system if you choose to add another tunnel.



    The host entered in the Fully Qualified Host Mapping field reads `exchange2.example2.com`.

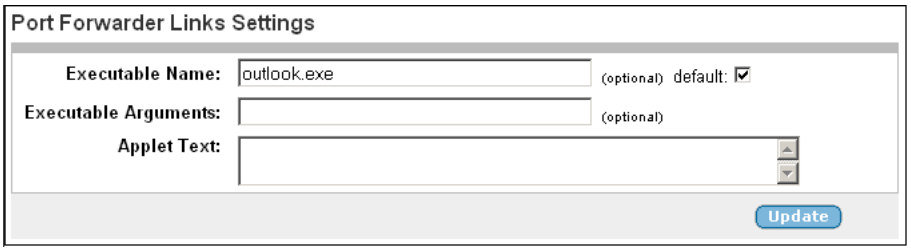
21. Click **Update**.
22. In portal Link form, click on **General** tab.

    The Outlook Port Forwarding Links form appears.
23. Enter the application specifics.

    By selecting the default check box, outlook.exe is suggested as executable in the Executable Name field.

    If desired, enter arguments to the Outlook client in the Executable Arguments field. An example of an argument can be /Profile myprofile.

    For a reference to available Outlook arguments, see Microsoft Knowledge Base Article no 296192 available on http://support.microsoft.com/?kbid=296192



24. In the **Applet Text** field, enter a custom text (for example with user instructions) to be displayed in the Java applet window (optional).

    See example 7a for a more detailed description of this step.
25. Click **Update**.
26. In the System tree view, expand VPN Gateways and Gateway Setup and select **DNS**.
27. In the **Search List** field, configure the Exchange servers' domain name suffixes as DNS search entries for the portal server.

    This step is absolutely necessary for the Outlook Port forwarder to work. Using the Exchange servers exemplified in 17 on page 158 and 20 on page 158, the following domain names can be entered.
28. Click **Update** and apply the changes.

Port Forwarder API

The AVG software provides an API for developing a custom application that automatically logs in the user to the desired VPN and executes a previously configured Port forwarder link on the Portal's Home tab. This way, a remote user does not have to browse to the Portal and click the Port forwarder link to set up the required application tunnel(s).

Briefly, this is how to use the Port forwarder API.

1. Configure a Port forwarder link of the desired type.
2. Develop a Java application/applet that uses the Port forwarder API.

   The Port Forwarder API can be downloaded from the Portal through the URL `https://vpn.example.com/avaya_cacheable/portforwarder.zip`, where `vpn.example.com` is the DNS name of your Portal. API programming instructions and examples in Appendix I in the *User's Guide*.

Example 9: HTTP Proxy Link

Like the **internal** link, the **proxy** link lets the user access web pages through a secure SSL connection. However, a web page may contain plugins (for example a Flash movie) which, in their turn, may include embedded links to other web pages. If a user executes such an embedded link, the HTTP request may not reach the VPN Gateway and the URL will not be displayed.

To ensure display of all URLs – also ones that are embedded in plugins – the HTTP Proxy feature lets the user download a Java applet to the client. The client browser's proxy settings should then be changed to direct all HTTP requests to this Java applet. The Java applet in its turn routes each request through a secure SSL tunnel to the VPN Gateway 's proxy server, where it is unpacked and redirected to its proper destination.

For users with Internet Explorer, the link can be configured to change/clear the proxy settings automatically.

Note:

Outlook Port forwarder links (if configured) or Outlook Port forwarder portal sessions (Advanced tab) will not work if a proxy server is configured in the client browser.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
2. Click on the VPN Gateway name.

   VPN Summary screen appears.
3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.
4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

   The Add New Linkset form appears.
6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example `<b>Heading</b>` for a boldface heading.

   In the following example, the FONT tag (`<FONT FACE="Impact">File server access</FONT>`) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

    Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the text `HTTP proxy link`.

13. In the **Link Type** list box, select the desired link type, that is **HTTP Proxy**.
14. Click **Continue**.

    The form is expanded.

15. In the **Update Client Link Proxy Settings** list box, select whether or not to reconfigure the clients browser's proxy settings.

    If you select **yes** here, the user does not have to reconfigure the browser's proxy settings manually. They are automatically reconfigured to use 127.0.0.1 and 4567 as proxy server address and port. This is specified for both HTTP and HTTPS (Secure) traffic in IE's Proxy settings window. When the user exits the Java applet window, the proxy settings are automatically restored to the original settings.

    Note that automatic updating and clearing of the proxy settings are only possible for Internet Explorer running on Windows.

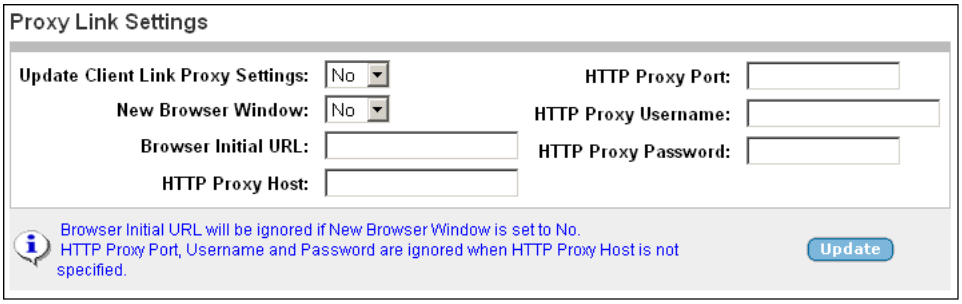
    If set to **no**, or if another browser than Internet Explorer is used (for example Netscape), instructions on how to reconfigure the proxy settings manually is provided in the Java applet window displayed when the user clicks the HTTP Proxy link.

16. In the **New Browser Window** list box, select whether or not to open a new browser window.

If you select **yes** here, a new browser window will automatically be opened when the user clicks the HTTP Proxy link. If set to **no**, the user should open a new browser window to start browsing in HTTP Proxy mode.

17. In the B**rowser Initial URL** field (optional), specify the URL to be opened.

    This field will be ignored unless you chose to open a new browser window (see the previous step). When you enter the URL, also specify the protocol, that is http or https, for example `http://www.example.com`.



18. In the **HTTP Proxy Host** and **Port** fields, enter the address and port of an intermediate HTTP Proxy server (if any).

    If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

    Skipping these fields means that all applet traffic will be tunneled directly to the AVG, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.

19. If an intermediate HTTP Proxy server is specified, enter the credentials to access this server (if required).

    These fields will be ignored if the previous step was skipped.

20. Click **Update**.

21. Apply the changes.

    To access a web page in HTTP Proxy mode, the remote user should first click the link to download the HTTP Proxy applet, then reconfigure the browser's proxy settings (instructions are provided in the Java applet window). For users with Internet Explorer, the link can be configured to change/clear the proxy settings automatically.

    Finally, the user should open a new browser window to start browsing in HTTP Proxy mode. As an alternative, the link can be configured to open a new browser window automatically.

    To quit surfing in HTTP Proxy mode, the user should click the Stop Port Forwarder button in the Java applet window and manually restore the original browser settings.

Note that this last step is not required if the link is set to configure/clear the browser's proxy settings automatically.

Example 10: FTP Proxy Link

To enable access to an FTP server through a native FTP client (installed on the remote user's machine), a Portal link can be created. When the user clicks the link, a Java applet is downloaded. The Java applet is instructed to listen to a port number on the user's own computer (that is 127.0.0.1 or any other IP address within the 127.x.y.z range).

The Java applet forwards all incoming traffic to a specified remote FTP server. The FTP client (if specified) will be started automatically on the remote user's machine and connect to the local IP address on the client machine. The AVG will then act as an FTP Proxy and relay data from the FTP client to the remote FTP server.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Click on the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, click on **Linksets**.

   The Portal Linksets form appears.

4. If Portal Linkset is already present go to Step 10.
5. Click **Add**.

   The Add New Linkset form appears.

6. In the **Name** field, enter the name of the current linkset.

   The linkset name should later be used to map the linkset to a group. In this example we will call the linkset files.

7. In the **Text** field (optional), enter a heading for the linkset.

   By entering a linkset text, a heading will be displayed on the Portal's Home tab. The heading will be placed just above the links included in the linkset. Any HTML source can be used to format the heading, for example Heading for a boldface heading.

   In the following example, the FONT tag (<FONT FACE="Impact">File server access</FONT>) has been used to format the heading with the Impact typeface. The heading File server access will be displayed above the SMB and FTP links.

8. Click **Update**.
9. Apply the changes.
10. Click on the Portal Linkset name and then on **Portal Links** tab.

Portal Links form appears.

11. Click **Add**.

    The Add Portal Links form appears.

12. In the **Text** field, enter the clickable link text to appear on the Portal's Home tab.

    In this example we will enter the text FTP proxy link.

13. In the **Link Type** list box, select the desired link type, that is FTP Proxy.

14. Click **Continue**.

    The form is expanded.

15. In the **Local Host IP** field, enter the local host IP address.

    The SSL tunnel will be established between the user's local machine (local host IP=any IP address within the 127.x.y.z range) and the VPN Gateway VPN Gateway.

16. In the **Local Port** field, enter the local TCP port.

    When specifying the local TCP port, use port numbers just above 5000, which are usually free to use, or use the application-specific port number for FTP file transfer, that is 21. On Windows machines any port number can be used.

17. In the **Remote FTP Server** field, specify the FTP server (IP address or host name).

    The VPN Gateway will relay data from the user's local machine to the specified target, that is the remote FTP server.

18. In the **Remote FTP Port** field, enter the remote port number.

19. In the **Application Path** field, specify the application to be started (optional).

    This step defines the application to be started when the user clicks the link. Enter the path to the FTP client, for example `c:\program files\application \app.exe`.

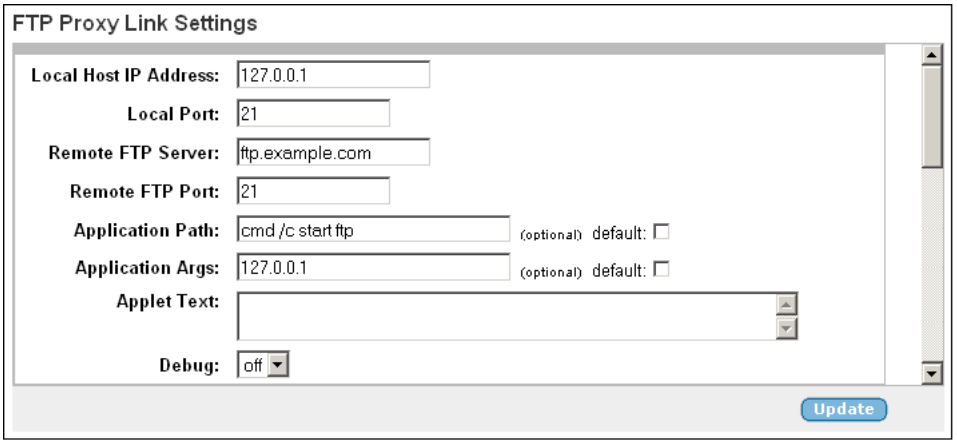
    By default, `cmd /c start ftp` is suggested, which means that the FTP session will be run in the command window.

    If it is preferred that the user starts the application manually, you can clear the application path. In this case, the remote user should click the link to start the FTP proxy, start the FTP client and connect to the local host IP address specified in.

20. In the **Application Args** field, specify an argument to the application (optional).

    This step identifies the command-line argument to be used by the application (if specified in the previous step). Note that each FTP application has its own set of arguments. See the documentation for the FTP client to be started with the FTP Proxy link.

The default argument tells the application (see the previous step) to connect to the local host IP address and port we specified in 15 on page 164.



21. In the **Applet Text** field (optional), enter a custom text to be displayed in the Java applet window.

    The custom text (if entered or pasted) will be displayed in the Java applet window that is automatically displayed when the user clicks the link. The text may for example include user instructions explaining the purpose of the FTP Proxy, how to start the FTP client and connect to the local host IP address.

22. Click **Update** and apply the changes.

Net Direct Link

Instructions on how to create the Net Direct link in Net Direct on page 171.

Chapter 9: Virtual Desktop

Virtual Desktop is an environment to access secure Web-based applications and services. Symantec On-Demand Agent (SODA) provides the Virtual Desktop environment so that the user can access confidential information in a secure environment.

Running the Virtual Desktop on Client Computers

The Virtual Desktop runs on computers meeting the following specifications:

- Pentium 633MHz or faster
- 128 MB RAM
- 25 MB MINIMUM available hard disk space required for Agent to download

Note:

More space may be required for your system to run smoothly after Agent is downloaded, because user data files must be virtualized for successful launch of certain applications.

- Windows Server 2003, Windows 2000 Pro, Windows 2000 Server, Windows XP, Windows NT4 (SP6)
- Browser: Internet Explorer 5.0 or later, Netscape 6.0 or later, Opera 7.2 or later, FireFox 1.0 and later
- Java Runtime Environment (JRE) version 1.4.2 or later, or Microsoft Java Virtual Machine (JVM) version 5.0 and later

Licensing vdesktop

The virtual desktop licenses are available in the volumes of 50,100, 250, 500, 1000, 2000, and 5000.

To activate the virtual desktop feature, you need to paste the license key for the same. Follow these steps, to paste the license:

1. Logon as admin.
2. Select **Config** tab.
3. In the system tree view, select **Host(s)**.
4. Click on SSL VPN Host name.

System Information screen appears.

5. Click on **Licenses** tab.
6. Paste the contents of the license.
7. Click **Save**.

Configure Security Settings

Once the desktop license is installed, you can define specific actions for it. You can allow users to print and to copy information to removable USB media, while in the Other location you can force users to work only within the Virtual Desktop (Enable Automatic Switch) and to work with copies of the files rather than the 'real' versions (Enable File Separation). You may also want to terminate the Virtual Desktop when the browser session is terminated to ensure that the Virtual Desktop session does not remain active indefinitely on halted or shared machines. You can configure these security settings using CLI or BBI.

For more information about configuration of security settings using BBI see, *Avaya BBI Application Guide*.

For more information about configuration of security settings using CLI see, *Avaya CLI Application Guide*.

Set Virtual Desktop in Portal

You need to specify the link type as virtual desktop to set the virtual desktop in the portal. Follow these steps to specify the linkset:

1. Logon as admin.
2. Select **Config** tab.
3. In the system tree view, select **VPN Gateways**.
4. Click on the VPN Gateway name.

   VPN Summary screen appears.
5. Select Link sets settings.
6. Click on the portal linkset in the table.

   Portal Linkset Configuration screen appears.
7. Click on **Portal Links** tab.
8. Click **Add**.
9. Specify an identifier for the link.

10. Specify the link text that appears on the Portal Web page, automatically displayed after a mobile user successfully logs in to the Portal.
11. Select the linktype as **Virtual Desktop**.
12. Click **Continue**.
13. Click **Apply** to apply the changes.

Chapter 10: Net Direct

About the Net Direct Client

Net Direct is a VPN client that can be temporarily downloaded to the client PC from the Web Portal. When the user exits Net Direct or the VPN session, the client is automatically uninstalled. Combined with Avaya Endpoint Access Control Agent and/or extended profiles, the Net Direct client offers a simple and secure access method.

Net Direct includes a network driver that captures network traffic and tunnels it through SSL to the AvayaVPN Gateway (AVG). The AVG then decrypts the traffic and forwards it to the requested destination. Which network destinations should be tunneled is configurable. The Net Direct client is packet-based, whereas the SSL VPN client (see Transparent Mode on page 263) uses system calls. Because the Net Direct client thus operates on a lower network level, it supports more applications, for example Microsoft Outlook and the ability to map network drives.

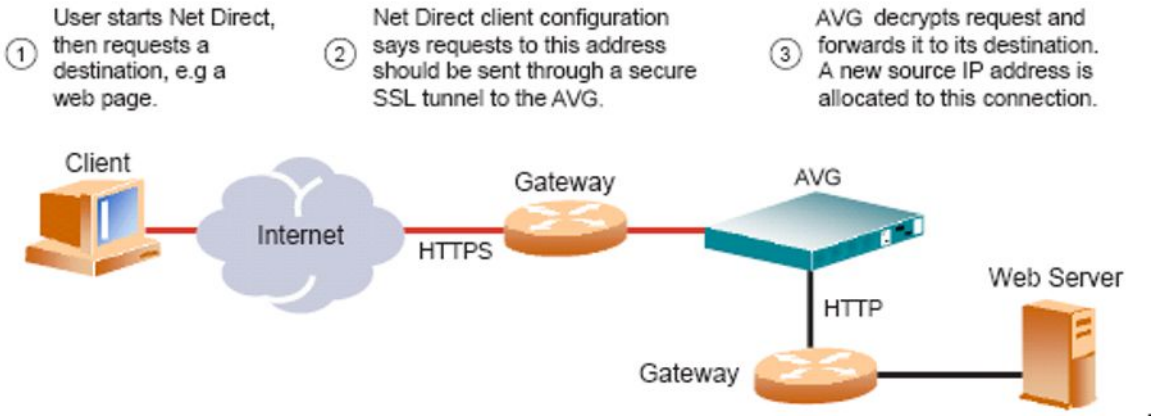


Figure 1: Net Direct Client Connection

Supported Operating Systems

Net Direct is supported on Windows, Linux, and Mac OS X (for PowerPC).

On Windows, the end user must be administrator user on his/her PC (or know the administrator password) to be able to download/install the Net Direct client. The Local administrator user name and password can however be stored on the AVG on a per group level. For remote users who are members of a group for which a valid Local administrator user name and password

have been stored, downloading and installing Net Direct is seamless. See Configure Local Administrator User Name/Password on page 184.

Downloading and installing Net Direct on Mac OS X requires the user to be member of the admin group. If the user is not a member of the admin group or enters the wrong password when prompted, he/she can log in with the root password as an alternative option. This in its turn requires that the user account is authorized to perform the command **`su root`**.

Downloading and installing Net Direct on Linux requires the user to be root user or see to it that the user account is authorized to perform the command **`su root`**. If the user is not running as root when attempting to download Net Direct, a window is displayed prompting the user for the root password.

Refer to the Release Notes for more detailed information, for example supported browsers, Java versions and limitations.

Net Direct Modes

The Net Direct client is available in three different versions, or modes:

- Downloadable client
- Cached client (Windows only)
- Installed client (Windows only)

Downloadable Client

By clicking a link on the Web Portal, the Net Direct client is downloaded, installed and launched on the remote user's PC. While Net Direct is running in the background, the remote user can access intranet resources through his or her native applications – without the need to install VPN client software manually. When the user exits Net Direct or the Portal, the client is automatically uninstalled.

Cached Client

To cut down on network traffic and start-up time, a cached version of Net Direct is available as a configurable option. If caching is enabled, Net Direct leaves some components from the first installation on the client machine when the user exits Net Direct or the Portal session. These components will only be retrieved from the server anew when they become outdated. How to enable caching is described on 10 on page 179.

Installed Client

The Net Direct client is also available as a setup.exe file to be installed permanently on the remote user's machines. No Portal login is then required. The user logs in through the user

interface provided by the installable Net Direct client. Just like the downloadable and cached versions, the behaviour of the installable version of Net Direct is completely controlled by the server settings made for the VPN Gateway (see the following sections).

Installing the installed client requires administrator privileges. For instructions on how to create a Portal link for downloading the installed version of Net Direct, see Configure Link for Downloading Installed Version on page 185.

When connecting to the AVG, the system checks the version of the installed Net Direct client. If a more recent version is available, the user will have to option to go to a web page where the new version of the client can be downloaded.

Mobility

If the connection is lost during a NetDirect user session, the NetDirect device still remains in UP state because client enters into the roaming mode and will preserve the session till the roaming time expires. You can configure the following NetDirect parameters on per VPN per Group:

- roaming mode
- roaming time
- list of networks on which roaming is allowed

During roaming time, it can roam through any physical interface which is in the configured roaming networks.

This allows the user to maintain the VPN session in cases like:

- A Wifi User roaming from one access point area to another access point or a subnet
- A user migrating from 802.3 ethernet environment to Wifi
- Temporary lose of connectivity to the server, due to an intermediate router or switch failure
- A Wifi user temporarily losing connectivity

This feature is supported on Windows, Linux and MAC. It is also supported on portal version of NetDirect as well as NDIC.

Server Configuration

In short, server configuration consists of creating one or several IP pools, enabling Net Direct, making the desired adjustments to default values (if needed) and configuring a Net Direct link.

Create IP Pool

The IP pool comes into play when the remote user tries to access a host using Net Direct. A new IP address has to be assigned as source IP for the unencrypted connection between the VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

Several IP pools can be configured, each with a unique ID number and unique properties. By mapping the desired IP pool to a user group, you can create different methods for IP address and network attributes assignment for different user groups.

One of the configured IP pools should be selected as the default IP pool. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

The IP pools are used to assign IP addresses for IPsec access (using the Avaya IPsec VPN client) as well (see Transparent Mode on page 263). If you have already configured an IP pool for use with the IPsec VPN client, this pool can also be used for the Net Direct client.

1. Log in to the BBI as VPN administrator user.
2. In the System tree view, expand VPN Gateways and Gateway Setup.
3. Select **IP Pool**.

   The IP Pool form appears.
4. Under IP Pool List, click **Add**.

   The IP Pool Configuration form appears.

   The first available IP pool number is suggested in the IP Pool ID list box.
5. In the **Name** field, enter a name for the IP pool.

   By giving the IP pool a suitable name, it will be easier to recognize when selecting it in other forms.
6. In the **Status** list box, select **enabled** to enable the IP pool.

   If needed, you can later disable this particular IP pool without losing the other settings for the pool. When appropriate, you can then reenable the pool without having to configure all settings once again.
7. In the **Type** list box, specify how IP address and network attributes should be assigned to the client.

   Network attributes (including IP address) can be assigned either locally (using free IP addresses from your local subnet), from a RADIUS server or from a DHCP server.

   For IP pools of the local type, network attributes should be configured on the AVG(see next section). For IP pools of the radius and dhcp types, network attributes can be configured on the AVG as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute.

8. If needed, change the default proxy ARP setting.
   - on: Means that the VPN Gateway that handed out the IP address for a specific client connection will respond to ARP requests on behalf of the Net Direct client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.
   - off: Return traffic will not be able to reach its destination unless specific routes are configured.
   - all: Same as on but proxy ARP is used on all interfaces.
9. Click **Update**.

   Depending on which pool mechanism (local, radius or dhcp) you have selected, the IP Pool Configuration form now displays different input fields. Follow the relevant description depending on your choice.

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism to **local** (as described in 7 on page 174 in the previous section), you should configure the desired IP address range. You can also configure network attributes to be retrieved from the system when the client connects.

If you set the source of IP assignment to **radius** or **dhcp**, continue with the relevant section (see the following pages) instead.

1. In the Lower IP and Upper IP fields, configure an IP address range.
2. Click **Update**.
3. Scroll down to Network Attributes Settings and configure the desired network attributes settings (optional).

   The Net Direct client normally works fine without specific network attributes. You can however specify the desired network attributes in the form if needed.
   - **Client Netmask**: Sets the network mask for the client. The network mask should cover the IP address range specified in 1 on page 175. The default network mask is `255.255.255.0`.
   - **Primary/Secondary NBNS server**: Sets the IP address of a primary NBNS server (NetBIOS Name Server). Used if the Net Direct client should use a specific NBNS server to have computer names resolved into IP addresses. NBNS servers provide WINS (Windows Internet Naming Service) which is part of the Microsoft Windows NT server environment.
   - **Primary/Secondary DNS server**: Sets the IP address of a primary DNS server. Use this command if the Net Direct client should use a specific DNS server to have domain names resolved into IP addresses. If no (primary or secondary) DNS server is specified here, the DNS server specified for the VPN

to which the remote user belongs will be used. This is configured under **VPN Gateways>Gateway Setup>DNS**. (This option is only possible if a Secure Services Partitioning license is loaded). If only a default DNS server is specified (under **Network>DNS**), this will be used.

- **Domain name**: Lets you specify the name of the domain used while a Net Direct tunnel is connected. It ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

4. Click **Update** and apply the changes.

Configure Retrieval of Network Attributes from RADIUS

If you set the IP pool's mechanism for network attributes assignment to radius, you should configure the system to retrieve network attributes from a RADIUS server.

How to configure a RADIUS server (including network attributes) is described in Authentication Methods on page 75.

A minimum requirement is to configure retrieval of client IP address and primary DNS server. You can retrieve a number of network attributes, for example primary/secondary DNS server, primary/secondary NBNS server and so on .

Network attributes can also be configured on the AVG as fallback values if the RADIUS server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the local type (see 3 on page 175 on 3 on page 175 for instructions).

RADIUS group binding option

When the RADIUS server does not return a “GROUP class attribute”, the AVC user is bound to an IPsec Group ID and user access granted. In previous releases, authentication succeeds only if the Group matching option is disabled, but the AVC user is assigned to an unmatched group or default group if any are defined. Otherwise, the login for the IPsec user is rejected with reason Access not allowed.

This feature is provided for AVC users who know their group name on AVG and the IPSec shared secret and who are not part of any group on LDAP server to connect successfully. With this feature enabled, RADIUS requests for user group information from the LDAP, and based on the defined policy, returns an empty class attribute to AVG allowing successfully connection.

About this task

Use the following procedure to set the RADIUS group binding option.

Procedure

1. Click the General Tab.
2. Select the RADIUS binding value from the RADIUS Group Binding pull-down menu.Enabled activates the feature.Disabled de-activates the feature.

Configure DHCP Settings

If you set the pool mechanism to dhcp (as described in the section Create IP Pool on page 174), you should configure the system to retrieve client IP address and network attributes from a DHCP server.

1. Under DHCP Servers, click **Add**.
2. Configure the external DHCP server IP address.
3. Click **Add**.
4. Apply the changes.

   Network attributes can also be configured on the AVG as fallback values if the DHCP server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the local type (see 3 on page 175 on 3 on page 175 for instructions).

Create Default IP Pool

One of the configured IP pools should be selected as the default IP pool. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

1. In the System tree view, expand VPN Gateways and Gateway Setup.
2. Select **IP Pool**.

   IP Pool form appears.
3. In the **Default IP Pool** list box, select an existing IP pool as the default IP pool.
4. Click **Update** and apply the changes.

Map IP Pool to User Group (Optional)

As mentioned on Server Configuration on page 173, several IP pools with different mechanisms (that is local, radius or dhcp) can be configured. By mapping the IP pools to different user groups you can provide different ways of assigning IP address and network attributes depending on the user's group membership.

It is not mandatory to map an IP pool to a group. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool. How to create a default IP pool is described in the next section.

This is how to map an IP pool to a user group:

1. In the System tree view, select **VPN Gateways**.
2. Click on the VPN Gateway name.
3. Under **Settings**, select **Groups**.

   The Groups form appears.
4. Click **Edit**.

   The Modify Group form appears.
5. In the **IP Pool** list box, select the IP pool that you wish to map to the current group.
6. Click **Update** and apply the changes.

   Members of the current group will now receive IP address and network attributes from the selected IP pool when connecting to the VPN using their Net Direct clients.

Enable Net Direct

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.
3. Under **Settings**, select **VPN Client**. Netdirect Client Access Settings screen is displayed. (insert ND_ClientAccess).
4. In the Net Direct Client list box, select the desired option.

   - **on**: Net Direct client access is enabled for all users in the current VPN, that is the client can be downloaded from the Portal provided a Net Direct link has been created on the Portal's Home tab.
   - **group**: Lets you delegate to group level whether or not Net Direct client access should be allowed. To enable Net Direct client access for members of a specific group, go to the **VPN Gateways >>VPN 1 »Group 1>>General** form, display the desired group and select **on** in the Net Direct client list box.
   - **off**: Net Direct client access is disabled.

   When Net Direct is enabled (that is set to **on** or **group**), the other fields and list boxes in the form become editable. Net Direct will work fine with the default settings so you do not normally have to change the settings (listed in 5 on page 179 to 11 on page 180):

5. In the Idle Check list box, select the desired option.

   - **on**: The Net Direct connection is terminated if the session is idle, when the user exits Net Direct, logs out from the Portal, reloads the Portal or closes the browser window. This is the default value.
   - **off**: The Net Direct connection is only terminated when the user exits Net Direct, logs out from the Portal, reloads the Portal or closes the browser window.

6. In the Rekey Traffic Limit field (optional), enter the desired value.

   This step sets the maximum traffic allowed (in Kbytes) before new session keys are exchanged between the Net Direct client and the VPN Gateway VPN Gateway. If desired, you can choose this option instead of the Rekey Time Limit option or combine both.

   The default value is 0, which disables the service. The field is only editable if Net Direct clients are allowed.

7. In the Rekey Time Limit field, enter the desired value (optional).

   This step sets the maximum lifetime (in seconds) of the single session key. The setting controls how often new session keys are exchanged between the Net Direct client and the VPN Gateway. Limiting the lifetime of a single key used to encrypt data is a way of increasing session security.

   The default value is 28800 seconds, that is 8 hours. A setting of 0 disables the service. The field is only editable if Net Direct clients are allowed.

8. In the UDP Ports field, enter the desired UDP port range.

   This step lets you configure UDP ports to be used by the Net Direct client. The Net Direct client will use configured ports for sending encrypted UDP packets to the VPN Gateway. If this fails (due to for example firewalls between the client and the VPN Gateway), the fallback is to use SSL.

   A range of at least two ports needs to be specified. The default port range is 5000-5001.

9. In the MSS Clamping list box, verify that the desired setting is selected.

   - **on**: The AVG clamps the MSS (maximum segment size) of a TCP SYN packet to the MSS of the real interface. This way packet fragmentation does not occur for TCP traffic, which optimizes the performance.
   - **off**: The AVG does not perform MSS clamping. Large encrypted packets from the virtual interface that do not fit into a single packet when sent to the server will be subject to fragmentation. This will result in a slower connection.

10. In the Caching list box, specify whether or not caching of Net Direct components on the client machine should be allowed.

    - **on**: Leaves some Net Direct components in the client machine's cache after the remote user has downloaded the Net Direct client from the Portal the first time. The next time the user clicks the Net Direct link, Net Direct will be installed and launched much quicker. When cached components are outdated, these will be fetched automatically from the Portal.

- **off**: All Net Direct components are removed from the client machine when the remote user exits the Portal session.

11. In the Operating Systems list, specify allowed operating systems.

    This command lets you filter out untrusted operating systems (OSs) in the remote user's client PC environment. If the OS is not present in the Selected list, the Net Direct client is not allowed to connect to the VPN Gateway VPN Gateway. The default value is **all**, that is no restrictions apply.

    - **all**: All Net Direct client connections are allowed, irrespective of what OS the client runs on.
    - **unknown**: Net Direct clients running on an OS that cannot be identified (for example new OS versions) are allowed to connect.
    - **winxp**: Net Direct clients running on Windows XP are allowed to connect.
    - **win2k**: Net Direct clients running on Windows 2000 are allowed to connect.
    - **generic_win**: Net Direct clients running on any other Windows version are allowed to connect.
    - **mac**: Net Direct clients running on Mac OS X are allowed to connect.
    - **linux**: Net Direct clients running on Linux are allowed to connect.

12. Click **Update** and apply the changes.

Banner Text

To configure a banner message to be displayed to the user when Net Direct is successfully downloaded and/or installed, proceed as follows:

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways form appears.

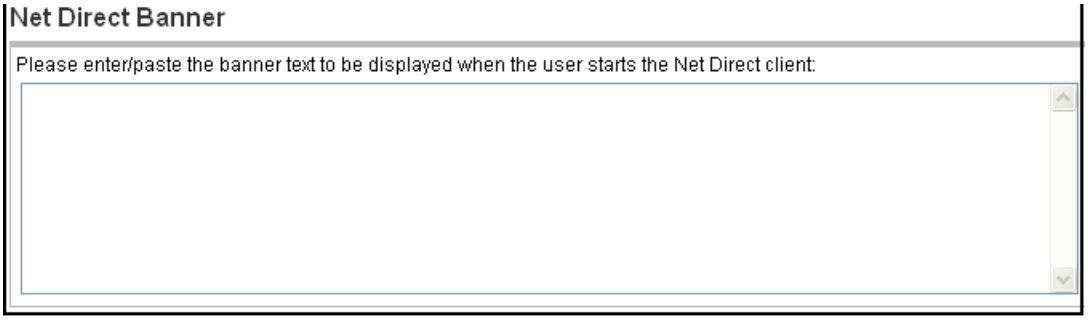
2. Select the name VPN Gateway.

   VPN Summary form appears.

3. Under **Settings**, select **VPN Client**.
4. Select **Net Direct Client**.

   Scroll down to the Net Direct Banner text box or click Net Direct Banner in the gray area.

5. In the text box, enter or paste the desired banner text.



6. Click **Update** and apply the changes.

   To view the result of the configuration done in this example, see the section Net Direct from a User Perspective on page 188.

   The banner text window will be displayed for the downloadable client as well as for the installed Net Direct client.

   If no banner text is configured, the window will not be displayed.

License Text

To display a window for the user to a accept or reject a Net Direct license agreement, enter or paste the desired text. If the user does not accept the license agreement, Net Direct exits.

Note:

A license text from Avaya is supplied by default. By entering a new license text, you will replace the default license text. If desired, you can copy and save the default license text before replacing it.

If you do not want the License agreement screen to be displayed at all, simply clear the **Net Direct License** text box.

Note:

By suppressing presentation of the Avaya Software License Agreement you agree to accept the terms of the agreement on behalf of the users receiving the client software from you. If you do not wish to accept the license terms on behalf of the users, then do not suppress presentation of the agreement.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways form appears.

2. Select the name VPN Gateway.

   VPN Summary form appears.

3. Under **Settings**, select **VPN Client**.
4. Select **Net Direct Client**.

Scroll down to the Net Direct License text box or click Net Direct License in the gray area.

5. In the text box, enter or paste the desired license text.
6. Click **Update** and apply the changes.

   Also see the section Net Direct from a User Perspective on page 188.

   The license text window is not displayed for the installed Net Direct client.

Configure Split Tunneling

This step lets you set the desired split tunnel mode. Split tunneling allows network traffic to travel either through a tunnel to the VPN GatewayVPN Gateway or directly to the Internet.

1. In the System tree view, expand VPN Gateways and VPN Client.
2. Select **Split Networks**.

   The Split Networks form appears.
3. In the **Split Tunnel Mode** list box, select the desired split tunnel mode.
   - disabled. Tunnels all network traffic through the Net Direct client to the VPN Gateway.
   - enabled. Tunnels traffic to

     specified networks (see the next step) to the VPN Gateway. All other network traffic goes through the computer's normal network interface.
   - enabled_inverse. Does not tunnel traffic to specified networks (see the next step), that is traffic goes through the computer's normal network interface. All other network traffic is tunneled through the Net Direct client to the VPN Gateway.
   - enabled_inverse_local. Does not tunnel traffic to directly connected networks or to specified networks (see the next step). This will for example allow the remote user to print locally, even while tunneled to the VPN GatewayVPN Gateway. All other network traffic is tunneled through the Net Direct client to the VPN Gateway. This is the default setting.

Note:

The Mac OS X modes `enabled_inverse` and `disabled` do not tunnel the local net`enabled_inverse` tunnels all network traffic through the Net Direct client to the VPN Gateway. This mode is not supported on Linux. If the user is running Net Direct on Linux or Mac OS X and the split tunneling mode is not supported, the `enabled_inverse_local` does not tunnel traffic directly connected network and configured network

4. Click **Update**.

   Unless the split tunnel mode is set to disabled, continue with specifying the network addresses to be tunneled (or not tunneled if any of the inverse modes have been selected).

5. Under Split Tunnel Network List, click **Add**.
6. In the Network IP field, enter the network IP address to be tunneled.
7. In the Network Mask field, enter the desired network mask.
8. Click **Update**.
9. Add another network in the same way, by repeating 5 on page 183 to 8 on page 183.
10. Apply the changes.

Configure Net Direct Link

1. In the System tree view, expand VPN Gateways and select **Portal Linksets**.

   In the following steps we will create a portal linkset with a Net Direct link. Finally we will map the linkset to a user access group.

   You can also use an existing linkset. In the System tree view, expand Portal Linksets and select Links. In the Portal Links form, select the desired VPN and an existing portal linkset. Click Add. Then continue with step 10 on page 184.

2. Click **Add**.

   The Portal Linkset Configuration form appears.

3. In the **Name** field, enter a name for the linkset. for example netdirect.

   Using the linkset name, we will later map this linkset to a user access group.

4. In the **Text** field (optional), enter a heading for the linkset.

   The heading will be displayed on the Portal's Home tab, just above the links that are included in the linkset. Note that HTML formatting can be used in the Text field, for example heading to create a boldface heading.

5. In the **Autorun** list box (optional), make the desired selection.

   With autorun set to true, all links defined for the linkset will be executed automatically when the user enters the Portal after being successfully authenticated. In addition, these links will not be visible on the Home tab.

6. Click **Update**.
7. In the System tree view, expand Portal Linksets and select **Links**.
8. In the VPN Number and Portal Linkset list boxes, select the desired VPN and the linkset where you want to include the link. Click Refresh following each selection.

9. Click **Add**.

   The Portal Links form appears.
10. In the **Text** field, enter the clickable link text to be displayed on the Portal's Home tab, for example Net Direct.
11. In the Link Type list box, select the **Net Direct** link type.
12. Click **Continue**. On the next form, click **Update**.

    If you have added the link to an existing linkset and this linkset is already mapped to group, configuration is complete. Apply the changes. Otherwise continue with the next step.

Map Linkset to Group

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways form appears.
2. Select the name VPN Gateway.

   VPN Summary form appears.
3. Under **Settings**, select **Groups**.

   The Groups form appears.
4. Click **Add**.

   This step adds a new user access group to which the linkset (including the Net Direct link) should be mapped. For detailed information about how to create groups with access rules, see Groups, Access Rules and Profiles on page 35.

   You can also map the linkset to an existing group. In this case, skip this step and continue with the next step.
5. Expand Groups and select **Linksets**.
6. Verify that the correct group id/name is displayed in the **Group** list box.
7. In the **Portal Linksets** list box, select the linkset we have just created (that is netdirect) and click Add.
8. Apply the changes.

Configure Local Administrator User Name/Password

To be able to download and install the Net Direct client, users have to be administrators on their PCs. For users that are not administrators, you can store the local administrator user name and password in your VPN configuration. The credentials are stored per group.

This solution is suitable for larger companies, where the administrator account is identical for all or several of the employees' PCs. For successful installation of Net Direct, the administrator

credentials entered here must match those of the administrator account on the group members' PCs.

Note:

By supplying the Local administrator user name and password as described, the security in your Windows environment may be impaired. Carefully consider the risks before proceeding with this option.

1. In the System tree view, expand **VPN Gateways**, **Group Settings** and **Groups**.
2. Select **General**.
3. Verify that the desired VPN and group id/name are displayed in the VPN Number and Group list boxes, respectively.
4. In the **Net Direct Windows Admin User Name** field, enter the Local administrator user name.
5. In the **Net Direct Windows Admin Password** fields, enter the Local administrator password.
6. Click **Update** and apply the changes.

   When a user who belongs to this group logs in to the Portal and tries to download the Net Direct client on a PC that requires administrator privileges when installing new software, installation will be successful.

   Tip! Another way of solving the administrator requirement issue is to enable caching of Net Direct components. With caching on, Net Direct need only be installed by an administrator the first time the client is downloaded through the Net Direct link on the Portal's Home tab. After that, the user can download, install and run Net Direct whenever he wants. For instructions on how to enable caching, see 10 on page 179.

Configure Link for Downloading Installed Version

Follow these steps to create a portal linkset with a link for downloading the installed version of Net Direct.

1. In the System tree view, expand VPN Gateways and select **Portal Linksets**.

   If you wish to use an existing linkset instead, go to the System tree view, expand Portal Linksets and select **Links**. In the Portal Links form, select the desired VPN and an existing portal linkset. Click **Add**. Then continue with 7 on page 186.
2. Click **Add**.

   The Portal Linkset Configuration form appears.
3. In the **Name** field, enter a name for the linkset. for example installed_ND.

   Using the linkset name, we will later map this linkset to a user access group.

4. Click **Update**.
5. In the System tree view, expand Portal Linksets and select **Links**.

   The Portal Links form appears.
6. In the **VPN Number and Portal Linkset** list boxes, select the desired VPN and the linkset where you want to include the link. Click **Refresh** following each selection.

   In this example you should select the linkset we have just created, that is **installed_ND**.
7. Click **Add**.

   The Add Portal Links form appears.
8. In the **Text** field, enter the clickable link text to be displayed on the Portal's Home tab, for example **`Download Net Direct installation package`**.
9. In the **Link Type** list box, select the External Website link type.
10. Click **Continue**.

    The form is expanded.
11. Under External Link Settings, in the Protocol list box, select **https**.
12. In the **Host** field, enter the Portal's host name or IP address, for example vpn.example.com.
13. In the **Path** field, enter `/avaya_cacheable/NetDirect_Setup.zip`.
14. Click **Update**.

    If you have added the link to an existing linkset and this linkset is already mapped to group, configuration is complete. Apply the changes. Otherwise continue with the next step.

Map Linkset to Group

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways form appears.
2. Select the name VPN Gateway.

   VPN Summary form appears.
3. Under **Settings**, select **Groups**.

   The Groups form appears.
4. Click **Add**.

   This step adds a new user access group to which the linkset (including the Net Direct link) should be mapped. For detailed information about how to create groups with access rules, see Groups, Access Rules and Profiles on page 35.

You can also map the linkset to an existing group. In this case, skip this step and continue with the next step.

5. Expand Groups and select **Linksets**.
6. Verify that the correct group id/name is displayed in the **Group** list box.
7. In the **Portal Linksets** list box, select the linkset we have just created (that is **installed_ND**) and click Add.
8. Apply the changes.

Enable Full Access Tab

If not already active, the Net Direct client can be started from the Portal's **Full Access** page (select **Full Access** on the **Access** tab). This however requires that the Full Access feature is enabled.

For more information about starting the Net Direct client from the **Full Access** page, see The Portal from an End-User Perspective on page 287.

1. Follow the instructions for enabling Net Direct client access previously in this chapter.
2. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
3. Select the VPN Gateway name.

   VPN Summary screen appears.
4. Under **Settings**, select **Portal**.

   Portal General Settings screen appears.
5. Click on **Full Access** tab.
6. In the Status list box, select **enabled**.
7. Click **Update** and apply the changes.

NDIC configuration

NDIC configuration allows you to create a custom version of NetDirect_Setup.zip. This zip file contains pre-defined list of connection profiles and custom logo in the GUI. It is distributed from another web server or from AVG server itself as custom content.

To download this zip file from portal, follow these steps:

1. Place the customized setup (NetDirect_Custom_Setup.zip) file in a TFTP Server's root directory.
2. Login as user.
3. Type the command, `make-part-rw /isd on`.
4. Go to the directory, `/isd/isdssl/lib/portal-sys_7.*/priv/docroot/avaya_cacheable`.
5. Type '`tfp <tfp server ip>`.

   TFP prompt is displyed.
6. Type `bin` in TFP prompt.
7. Type '`get NetDirect_Custom_Setup.zip`' .

   This will import the customized NDIC setup in to AVG.
8. Type '`quit`' to exit from TFTP prompt.
9. Logout from TFTP server.
10. Type `https://vpn-ip/avaya_Cacheable/NetDirect_Setup_Custom.zip` in the Client PC.

    You can download the customized zip file.

Net Direct from a User Perspective

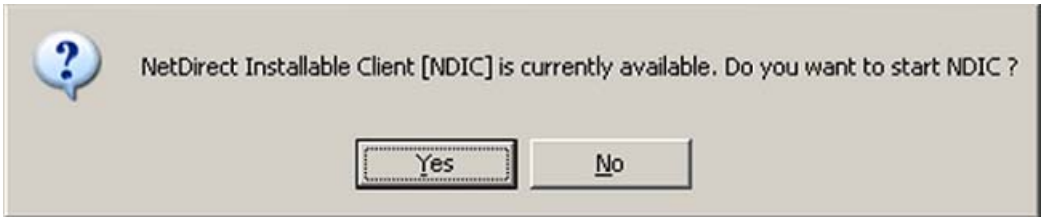
As mentioned previously, the Net Direct client can be downloaded temporarily from the Portal, to be used during a remote user's VPN session, or be installed permanently on the client machine. The following sections describe both scenarios.

Downloadable Version (Windows)

The downloadable version of Net Direct requires that a Net Direct link has been configured by the administrator (see Configure Net Direct Link on page 183). Consider the instructions as directed to the user.

1. Log in to the Portal.
2. Click the **Net Direct** link.

   If the installed Net Direct client (see Installed Version (Windows) on page 191) is already installed on the user's PC, the following message is displayed:



The installed version takes preference over the downloadable and cached versions.

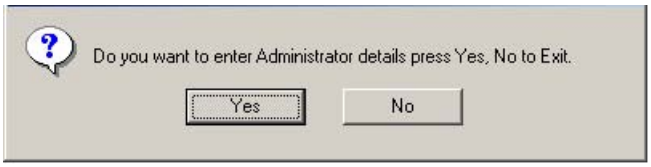
Click **Yes** to start the installed version of the Net Direct client. The Net Direct client window is displayed. Continue with the instructions on 8 on page 192.

If RIP Listener is activated on the client machine, a message is displayed. It warns the user that the connection can be interrupted if the client computer's routing tables are changed due to an RIP message. RIP Listener is a Windows component that can be disabled if required. For more information about RIP Listener, see Windows Help and Support Center.

3. Click **OK**.

   If the user has administrator privileges (which is required to install the Net Direct client), or if the Local administrator password is stored in the CLI for the group in which the user is member (see Configure Local Administrator User Name/ Password on page 184), a progress bar is displayed while the Net Direct client is being downloaded.

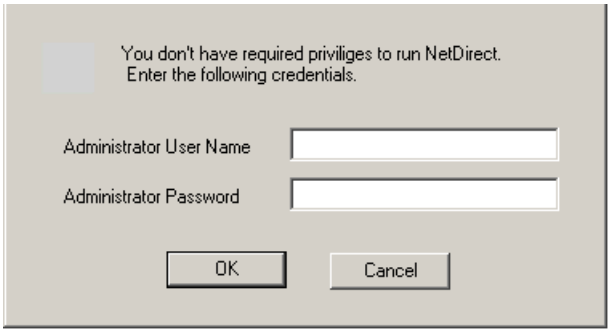
   If the user does not have administrator privileges on the PC, the following message is displayed:



4. Click **Yes** if you have access to the Local administrator user name and password for the PC.

   If you click **No**, the process of downloading Net Direct will be cancelled.

   The following window is displayed:



5. Enter the Local administrator user name and password and click OK.

   If Net Direct has been configured to display a license agreement window (see License Text on page 181), this is displayed.

6. If you accept the license terms, click I Agree to continue with the installation.

   A progress bar is displayed while the Net Direct client is being downloaded.

   Note:

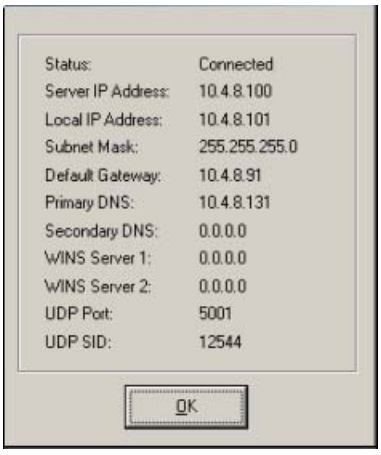
   The Net Direct client will not be started if the installable Avaya SSL VPN client or the Avaya IPsec VPN client (formerly the Contivity VPN client) is already running on the remote user's machine.

   If Net Direct has been configured to display a banner message window (see License Text on page 181), the Licence Agreement screen is displayed.

7. Click **OK**.

   When the Net Direct client is fully installed and has connected to the VPN server (that is the VPN Gateway), this is confirmed with an icon being displayed on the system tray.

   By right-clicking the system tray icon and selecting **Status**, connection details are displayed:



8. The user can now start the desired TCP- or UDP-based native application to connect to an application server on the intranet.

   Because the remote user has already authenticated to the Portal, no further login is required.

9. To exit the session, right-click the Net Direct icon on the system tray and select Exit.

   When the user logs out from the Portal, reloads the page or closes the browser window, the Net Direct client will exit and be removed from the user's machine.

   If errors should occur, the NetDirectError.log file is created under `C:\Documents and Settings\<user>\Local Settings\Temp` on the client machine.

Installed Version (Windows)

As an alternative to the downloadable, session-based version of Net Direct, a Net Direct client installation package can be downloaded from the Portal for the user to install Net Direct permanently on the client machine. This however requires that a download link has been configured by the administrator (see Configure Link for Downloading Installed Version on page 185). Consider the instructions as directed to the user.

1. Log in to the Portal.
2. Click the download link.

   A file download window is displayed.

3. Save the setup.zip file to your desktop.
4. Unzip the file.
5. Run the setup.exe installation package and restart your computer.

   This will install the Net Direct client permanently on your machine.

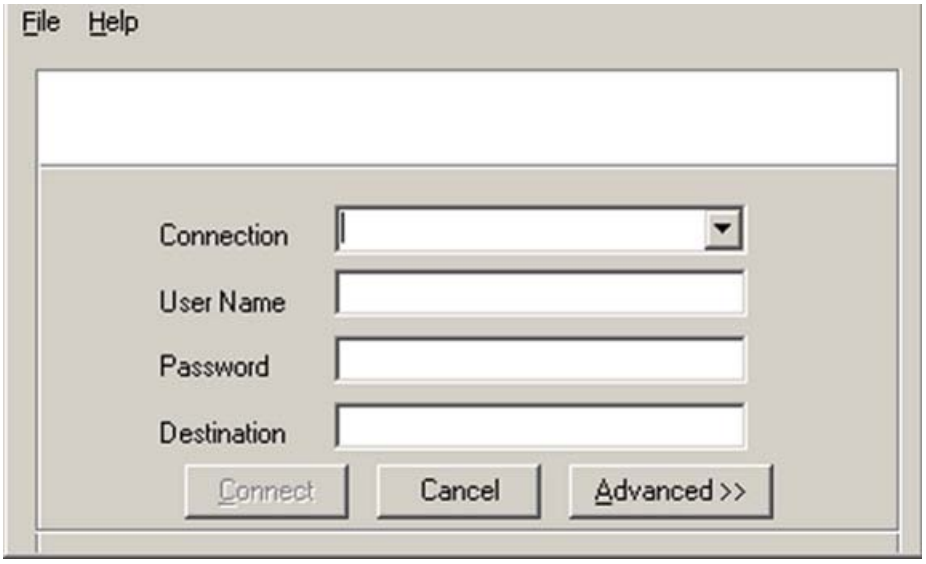
6. Start Net Direct.

   Double-click the **Avaya Net Direct Client** icon on your desktop or select **Avaya Net Direct** from the Start menu.

   If RIP Listener is activated on the client machine, a message is displayed. It warns the user that the connection can be interrupted if the client computer's routing tables are changed due to an RIP message. RIP Listener is a Windows component that can be disabled if required. For more information about RIP Listener, see Windows Help and Support Center.

7. Click **OK**.

   The Net Direct client window is displayed.



8. In the **Connection** field, enter a name for the connection, for example VPN 1.

   To select a previously saved connection, select the desired entry in the **Connection** list box. All fields except the Password field will be completed.

9. In the **User Name** and **Password** fields, enter the credentials given to you for login to the VPN.

10. In the **Destination** field, enter the IP address or DNS name to the VPN.

    IP address (if used) is the same as the Portal IP address. If DNS name is used, https:// need not be entered.

    Click **Advanced** to view some additional settings:

    - **Port**. Used if another port number than the default SSL port of 443 is used.
    - **Login Service**. Lets you select a specific authentication server to log in to (if configured).
    - **Save Settings**. Saves the login and destination details (except password). The information is presented as default values the next time you start Net Direct or, if several connections have been defined, selectable in the **Connection** list box.

    An alternative way of supplying and saving login details is to select **Connection Wizard** on the **File** menu and follow the steps.

11. Click **Connect**.

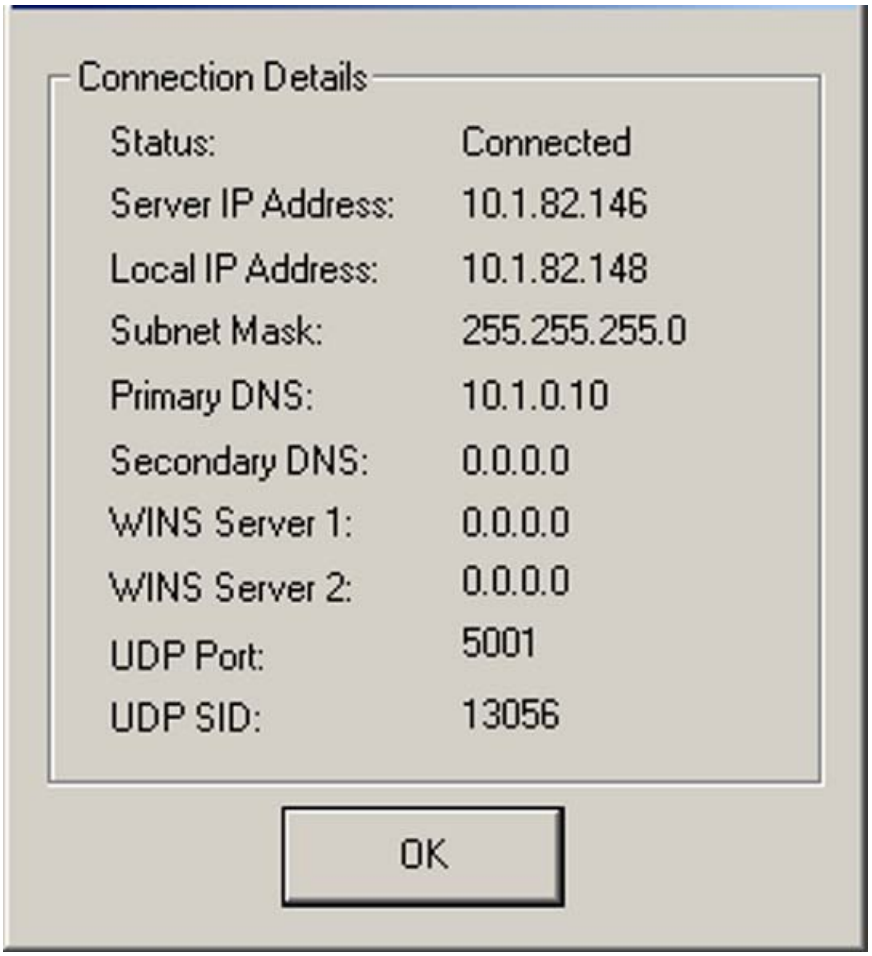
    When Net Direct has connected to the VPN server, the Net Direct client window is minimized and the Net Direct icon is displayed on the system tray.

    If Net Direct has been configured to display a banner message window (see License Text on page 181), the message is displayed.

12. Click **OK**.

    Three different statuses can be indicated by the Net Direct icon on the system tray:

    By right-clicking the system tray icon and selecting **Status**, connection details are displayed:



13. The user can now start the desired TCP- or UDP-based native application to connect to an application server on the intranet.

    Because the remote user has already authenticated to the Portal, no further login is required.

14. To exit the session, right-click the **Net Direct** icon on the system tray and select **Exit**.

    When the user logs out from the Portal, reloads the page or closes the browser window, the Net Direct client will exit.

    If errors should occur, the NetDirectError.log file is created under `C:\Documents and Settings\<user>\Local Settings\Temp` on the client machine.

When connecting to the AVG, the system checks the version of the installed Net Direct client. If a more recent version is available, the user will have to option to go to a web page where the new version of the client can be downloaded.

Downloadable Version (Mac OS X)

Only the downloadable version of Net Direct is available for Mac OS X. The downloadable version of Net Direct requires that a Net Direct link has been configured by the administrator (see Configure Net Direct Link on page 183). Consider the instructions as directed to the user.

1. Start Safari and log in to the Portal.
2. Click the **Net Direct** link.

   Because you have to be a member of the admin group (or know the root password) to download Net Direct, you are prompted for your password.

3. Enter your password and click **OK**.

   If the password is accepted, a Java applet window will be displayed (see next page). If you are not a member of the admin group, click **OK** without entering anything in the field. You will then be prompted for the root password in a second login window. If you enter the wrong password in the preceding dialog, you will automatically be redirected to the root password dialog.

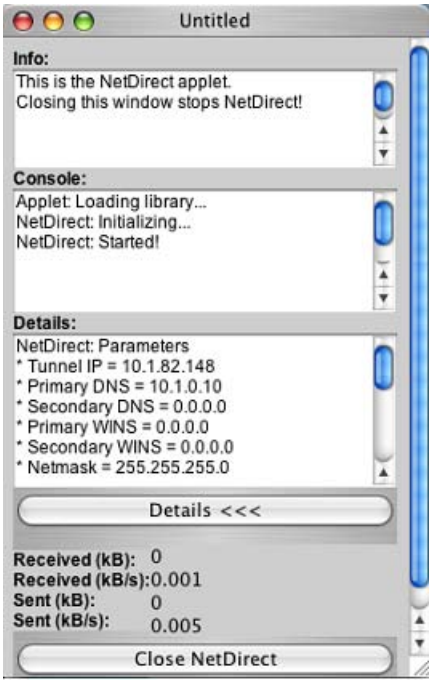
4. Enter the root password and click **OK**.

   If the password is accepted, a Java applet window will be displayed.

If you do not know the root password, Net Direct cannot be downloaded.

When the Net Direct client is fully installed and has connected to the VPN server (that is the VPN Gateway), this is confirmed in the Java applet window.

Click the **Details** button to display connection details:



5. The user can now start the desired TCP- or UDP-based native application to connect to an application server on the intranet.

Because the remote user has already authenticated to the Portal, no further login is required.

6. To exit the session, click the **Close Net Direct** button in the Java applet window.

   When the user logs out from the Portal, reloads the page or closes the browser window, the Net Direct client will exit and be removed from the user's machine.

   If errors should occur, the NetDirectError.log file is created under /tmp on the client machine. This is the same path as for Linux.

Chapter 11: Customize the Portal

This chapter explains how to customize the Portal with respect to logo, company name, color, static link texts and language version.

Default Appearance

The default appearance of the Portal is shown.

Figure 2: Default Appearance

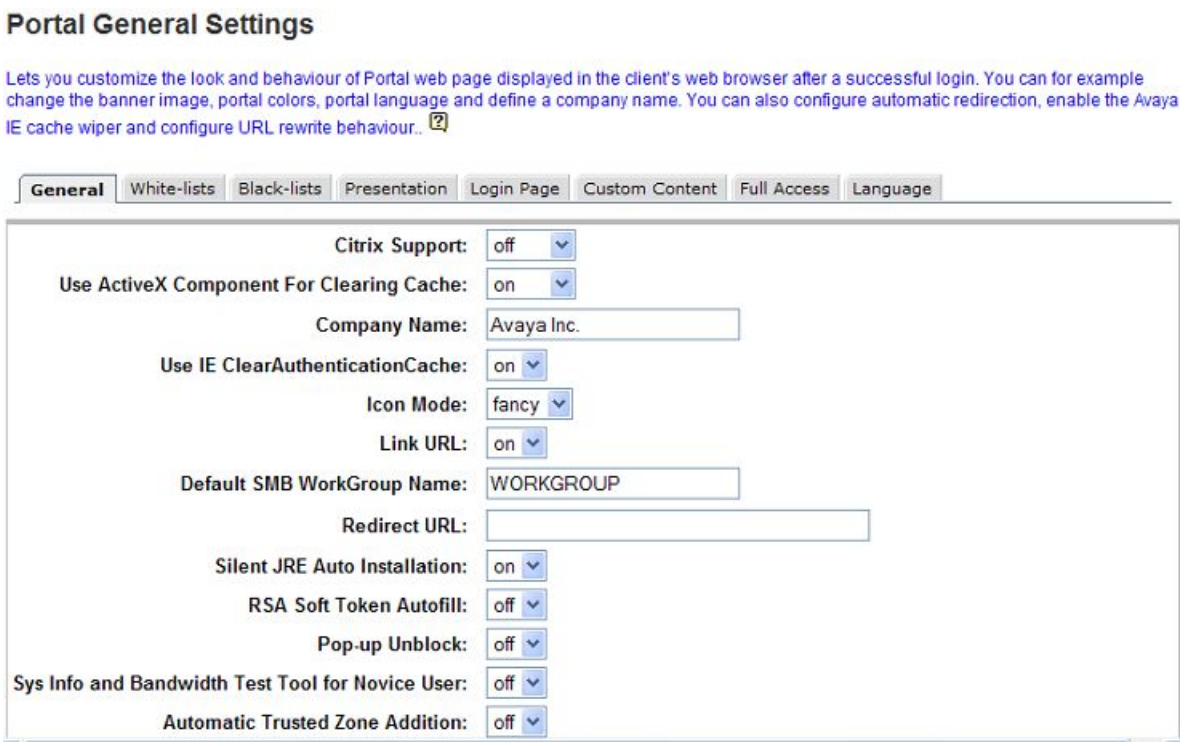
General Settings

The General Settings form lets you change a number of settings for the Portal.

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
3. Under settings, select the Portal.

   The Portal General Settings screen appears.



4. In the **Citrix Support** list box (optional), make the desired setting.

   - **on:** Enables support for Citrix Metaframe web links on the Portal. The Portal link is easily created by specifying the URL to the Citrix Metaframe server with the Internal Website or External Website link types.
   - **group:** Lets you enable/disable Citrix Metaframe support per user group instead of per VPN. Go to **VPN Gateways » VPN-1 » Group-1 » Modify Group** to enable or disable Citrix Metaframe support on group level.
   - **off:** Links to Citrix Metaframe servers are only supported if the link is created by means of the **custom** port forwarder link type. If Citrix Metaframe links are not used, **off** is the recommended setting, because this saves the AVG from starting the Java applet that supports this feature.

   Note:

   When **citrix** is set to **on** (on VPN level or group level), the AVG supports rewrite of ICA files only. Other methods are possible but may require configuration changes on the Citrix Metaframe server side.

5. In the Use ActiveX Component for Clearing Cache list box, make the desired setting.

   - **on:** The remote user – if running Internet Explorer – will have the option to download the Avaya IE cache wiper when logging in to the Portal. If downloaded, the cache wiper will clear the cache from HTML pages accessed during the Portal session. In addition, the Portal address is removed from the browser's visited URLs list when the Portal session is terminated or when the

browser is closed. Previously cached content and history entries will not be cleared.

- **group:** Lets you enable/disable the IE cache wiper per user group instead of per VPN. Go to **VPN Gateways » VPN-1 » Group-1 » Modify Group** to enable or disable the IE cache wiper on group level.
- **off:** The IE cache wiper cannot be downloaded by the user. To allow caching of documents, enable the **Document Caching** setting (under **VPN Gateways » VPN-1 » HTTP**). The cache will however not be cleared.

6. In the **Company Name** field, enter the desired company name.

   This name will replace the default "Avaya" company name shown as a "tool tip" when hovering the mouse pointer over the Portal banner (logo) and as the browser window name.

7. In the Use IE ClearAuthenticationCache list box, make the desired setting.

   This setting controls the use of the ClearAuthenticationCache feature available in Internet Explorer 6, SP 1 and later. The feature is used to clear sensitive information (passwords, cookies and so on) from the cache when a user logs out from a secure session.

   - **on:** The cache is cleared for all instances of the current IE process when the user logs out from the Portal. This means that if the user is logged in to another web site, he will be automatically logged out from that site.
   - **off:** The cache is not cleared until the user closes the browser.

8. In the **Icon Mode** list box, select the desired icon mode.

   - **fancy:** Multi-colored, shaded and animated icons are displayed.
   - **clean:** Simple icons using a single one color are displayed. The color used is the same as for active tabs and the active area (see Default Appearance on page 197).

9. Specify a default value for Windows workgroup for SMB (Windows file share) servers.

   The default value is suggested in the [Workgroup] field on the Portal's Files tab and when creating SMB links.

10. In the **Link URL** list box, make the desired setting.

    - **on:** The **Enter URL** field will be visible on the Portal's Home tab.
    - **off:** The **Enter URL** field will be hidden.

11. Enter the URL to redirect.
12. Click **Update** and apply the changes.

White-list Settings

One of the fundamental features of the VPN Gateway product is the act of rewriting HTTP requests to HTTPS. When the remote user enters a URL (for example `www.example.com`) in the Portal's **Enter URL** field, the request is automatically rewritten as `https://`

`vpn.example.com/http/www.example.com`, where vpn.example.com is the Portal's DNS name. This ensures that traffic is sent through a secure SSL connection, through the AVG. When the user clicks a web link on the resulting web site, this request will also be rewritten.

Enabling the whitelist and specifying whitelist domains is a way of limiting rewrites of requests to domains listed as whitelist domains. All other requests will pass directly to the destination, without passing the AVG.

If unqualified domain names are used (for example `inside` instead of `inside.example.com`) the request is always rewritten, even if the domain is not included in the whitelist.

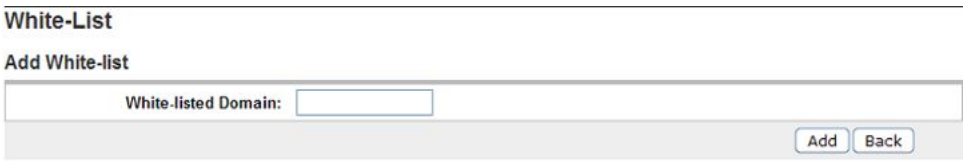
A typical usage can be to specify your intranet domains in the whitelist. The result can be that requests for Internet sites will be sent directly to the destination, without being rewritten whereas requests for the intranet domains will be sent through a secure SSL connection.

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN name from the Name list.

   The VPN Summary screen appears.
3. Under **settings**, select the Portal.

   The Portal General Settings screen appears.
4. Click on **White-List** tab.

   The White-list form appears.
5. Under **White-list Settings**, in the **URL Rewrite White-list** list box, select **on.**
6. Click **Update**.
7. Click **Add**.



8. In the **White-listed Domain** field, enter the domain to include in the white-list.

   Example: By entering `example.com`, all requests for URLs matching the example.com domain will be rewritten to include the AVG rewrite prefix (boldface):

   `https://vpn.example.com/http/www.example.com`
9. Click **Add**.
10. Click **Update** and apply the changes.

Black-List Settings

Using the Black-List form (VPN Gateways » VPN-1 » Blacklist), you can specify a list of domains to which requests should not be rewritten.

The system first checks the white-list to see if the request matches a domain listed there. It then continues to check the black-list to see if the request matches a black-listed domain.

Example: To rewrite all requests to **example.com**, except requests to the host **public.example.com**, specify example.com as a white-list domain and **public.example.com** as a black-listed domain.

Change the Presentation

To change the Portal's look and feel, proceed as follows:

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
3. Under settings, select the Portal.

   The Portal General Settings screen appears.
4. Select **Presentation**.

   A graphic representation of the Portal appears.

Change Color Theme or Individual Colors

1. To change the Portal's color theme, click **themes.**

   The Themes list box appears under the Portal graphic.

2. Select the desired theme and click **Update**.

   The color theme is applied to the graphic.

   Even though the Portal's individual colors can be changed (see next step), we recommend using color themes. Also consider how the applied color theme fits with the color of your company logo.

3. To change any of the four changeable Portal colors, click the **edit color** link shown next to (or on top of) the color.

   A color map is displayed.

4. Select the desired color in the map or enter a hexadecimal value corresponding to the color you wish to use.

   The hexadecimal value displayed in the field corresponds to the selected color. For a reference to some common colors and their hexadecimal color codes, see Table 2: Common Colors with Hexadecimal Color Codes. on page 204 .

5. Click **Update**.

Change Banner

1. To change the default banner (logo), click **edit banner** .

   The Banner field appears under the Portal graphic.

   Note that the size of the banner must not exceed 16 MB. If the cluster consists of several VPNs, the total size of imported banners in the different VPNs must not exceed 16 MB.

2. Click **Browse**.

   The folders in your file system are displayed.

3. Find the banner image you wish to use (in .gif format) and click Open.
4. Click **Update**.

   To restore the default banner, click **Reset**.

Edit Static Text

This will replace the default text that reads "This is a configurable text...".

1. To edit the static text, click **edit static text** .

A text field is displayed under the Portal graphic.

2. Enter the desired text and click **Update**.

Edit Number of Link Columns and Link Width

1. To edit the number of link columns, click **edit link columns** .

   The Number of Columns field is displayed under the Portal graphic.

2. Enter the desired number of columns for link display and click **Update**.

   To view the link column change, you have to apply the changes and connect to the Portal.

   If the number of link columns is set to 4, links 1 to 4 are placed on the first row, links 5-8 on the second row and so on . Additional links are added in sequential order from left to right on the next row. If for example link 2 is deleted, links 3-4 are adjusted left to fill the blank space, link 5 is moved up to the first row and links 6-8 are adjusted left.

   In the preceding example, the link area width is 100%, that is all of the white space is used.

3. To edit the link area width, click **edit link width**.

   The Width of Link Columns list box is displayed under the Portal graphic.

4. Select the desired percentage and click **Update**.

   To view the link width change, you have to apply the changes and connect to the Portal.

5. Apply the changes.

Hide Enter URL Field

To hide the Enter URL field displayed on the Portal's Home tab, proceed as follows:

1. Click **edit link url** .

   The following form appears:

2. In the Link URL list box, select **off** .

Common Colors

The following table lists a number of common web safe colors. For further reference, search the Internet for "web colors" and you will get access to sites with full reference to hexadecimal color codes.

Table 2: Common Colors with Hexadecimal Color Codes.

Color	Hexadecimal code
White	FFFFFF
Black	000000
Darkgray	A9A9A9
Lightgrey	D3D3D3
Red	FF0000
Green	008000
Blue	0000FF
Yellow	FFFF00
Orange	FFA500
Violet	EE82EE
Darkviolet	9400D3
Pink	FFC0CB
Brown	A52A2A
Beige	F5F5DC
Limegreen	32CD32
Lightgreen	90EE90
Darkblue	00008B
Navy	000080
Lightskyblue	87CEFA
Mediumblue	0000CD
Darkred	8B0000

Change Static Text on Login Page

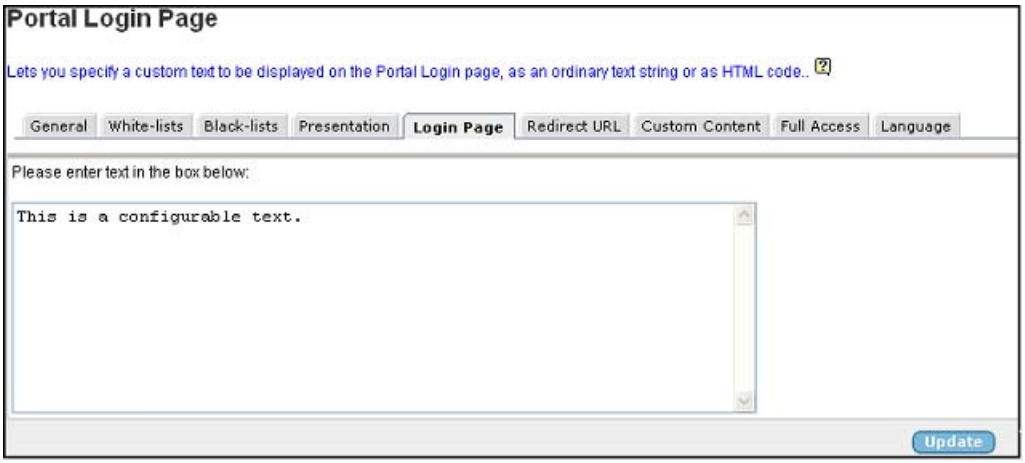
The static text displayed on the Portal Login Page can be changed as well. The default text is "This is a configurable text. ".

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
3. Under settings, select the Portal.

   The Portal General Settings screen appears.
4. Select **Login Page**.

   The Login Page form appears.



5. Enter the desired text in the text box and click **Update**.
6. Apply the changes.

Check the New Appearance

To check the new appearance of the Portal, connect to the Portal by entering the VPN's domain name in your browser. The default logo will be replaced on the Login Page as well as on the Portal.

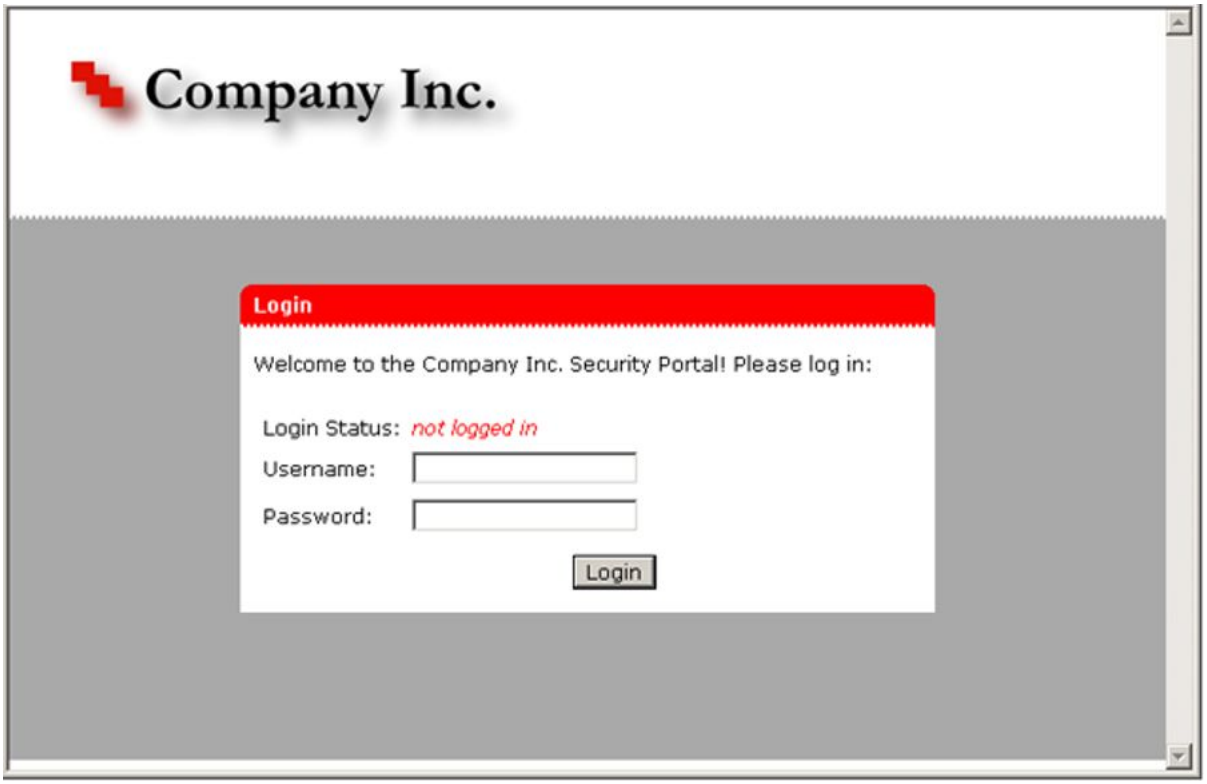


Figure 3: Login Page with New Logo, Colors and Static Text

After login, the Portal is displayed with a new logo, company name, static text and color.

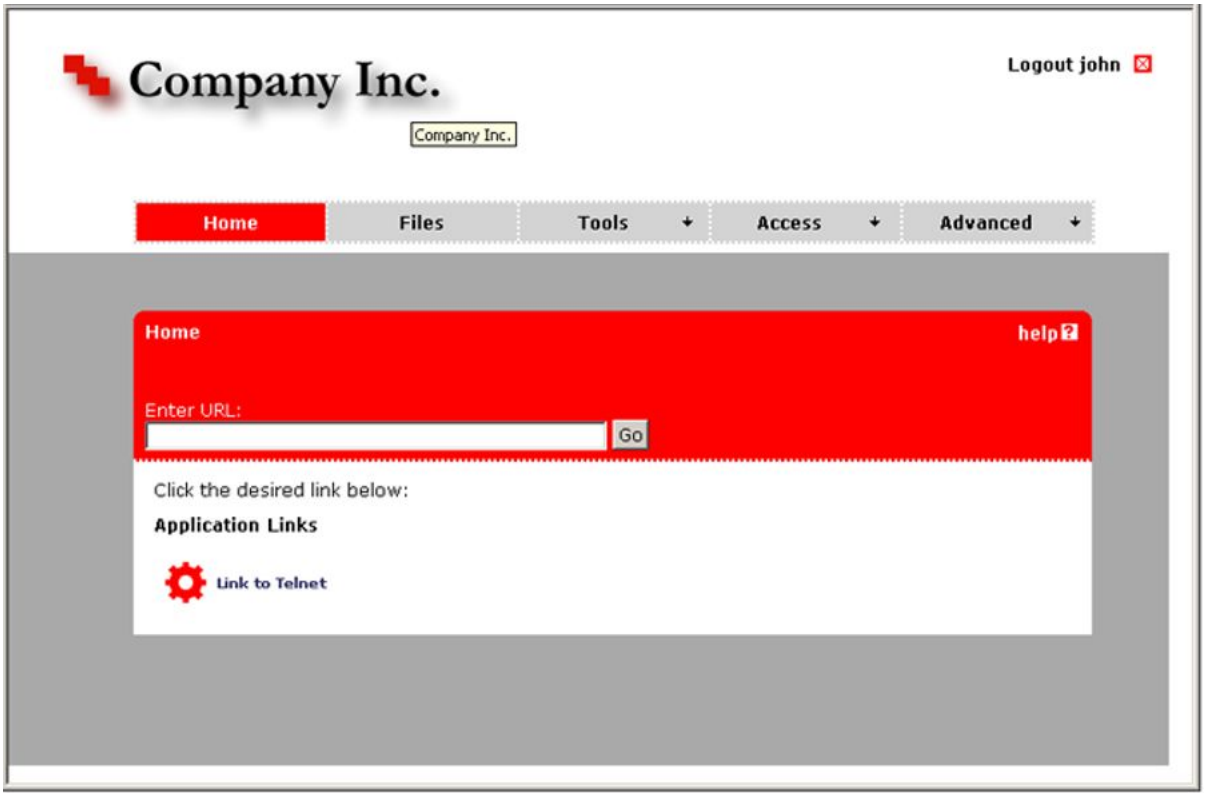


Figure 4: Portal with New Logo, Colors, Static Text and Company Name

Automatic Redirection to Internal Site

To automatically redirect a visitor to an internal site by passing the Portal altogether, proceed as follows:

1. Logon as Portal user.
2. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
3. Under settings, select the Portal.

   The Portal General Settings screen appears.
4. In the **Redirect URL** field, enter the desired URL.

   For redirection to work, the Portal address should be prefixed. Example: `https://vpn.example.com/http/inside.example.com`

   As an alternative, the *<var:portal>* macro can be inserted in the URL. The macro expands to the Portal's address. Example: `https:// <var:portal> /http/inside.example.com`
5. Click **Update**.

6. Apply the changes.
7. Insert a logout link on the internal site.

   For the visitor to be able to logout from the portal from the internal site, a logout link should be inserted on that page. This is what it might look like:

   ```
   <a href=https://vpn.example.com/logout.yaws> Logout from
   portal </a>
   ```

Automatic Redirection to Password-Protected Site

A visitor can be redirected to an internal password-protected site without a second login, provided the user name and password required on the intranet site is identical with the Portal's user name and password.

1. In the **Redirect URL** field, enter the URL to redirect the user to.

   Example: `https:// <var:portal> /http/ <var:user> : <var:password> @inside.example.com/protected`
2. Click **Update**.
3. Apply the changes.
4. Insert a logout link on the internal site.

   For the visitor to be able to logout from the portal from the internal site, a logout link should be inserted on that page. This is what it might look like:

   ```
   <a href=https://vpn.example.com/logout.yaws> Logout from
   portal </a>
   ```

Group-controlled Redirection to Internal Sites

Using the <var:group> macro, you may also redirect visitors to different internal sites, depending on their group membership.

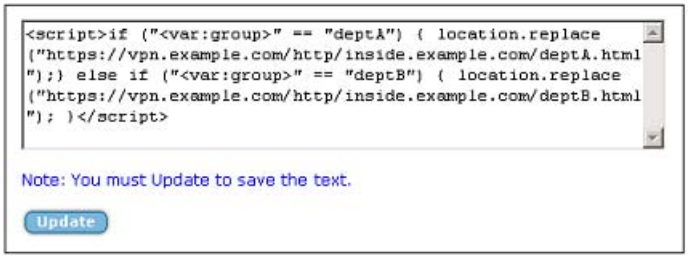
1. In the System tree view, select **VPN Gateways**.
2. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
3. Under settings, select the **Portal**.

   The Portal General Settings screen appears.
4. Select **Presentation**.

   The Portal Presentation form appears.
5. On the Portal graphic, click **edit static text.**

6. A text field is displayed under the Portal graphic.
7. Enter a script like the following:



   In the preceding example, deptA and deptB are group names.
8. Click **Update**.
9. Apply the changes.
10. Insert a logout link on the internal site.

    For the visitor to be able to logout from the portal from the internal site, a logout link should be inserted on that page. This is what it might look like:

    ```
    <a href=https://vpn.example.com/logout.yaws> Logout from
    portal </a>
    ```

    Note:

    In the same way, the <var:user> macro can be used to control the action taken depending on which user is currently logged in.

Change Portal Language

The SSL VPN software supports export of an English dictionary file whose entries can be translated to any language. Once translated, the file can be imported and set to replace the English language version on the Portal. Tab names, general text, button and field labels will thus display the imported file's language version.

Start by exporting the English language definition file.

1. In the System tree view, expand **Administration**.
2. Select **Operation**.

   The Host(s) screen appears.
3. Select **Language**.

   The Language form appears. Scroll down to Import/Export Language definition.

4. In the **Protocol** list box, specify the desired file transfer method.
5. In the **Server** field, enter the IP address of the file server to which you want to export the language definition file.
6. In the **File** field, enter a name for the language definition file, for example **`template.po`**.
7. If required, enter the desired credentials for FTP export in the **FTP User** and **FTP Password** fields.
8. Click **Export Language**.

   The next step is to translate the language definition file you have exported.

Translate Language Definition File

1. Open the language definition file with a text editor, for example Notepad.
2. Check that the **charset** parameter specified in the Content-Type entry is set according to the character encoding scheme you are using.

```
"Content-Type: text/plain; charset=iso-8859-1\n"
```

3. Translate the entries displayed under msgstr (message string).

   Do not translate the entries under **msgid** (message id). As you translate the file it may not be perfectly obvious where in the Portal your translation will turn up. If the text strings do not display where you expected (when the file is loaded to the Portal), simply edit the language definition file and reload it (see Import Language Definition File on page 211 Step).

```
#: portal.erl:764
msgid ""
" page."
msgstr ""

" pagina." <example in Spanish>
```

   There are very useful Open Source software tools for translating po files. You can find tools that run on Windows as well as Unix (search for **po files editor** in your web search engine). A translation tool is particularly useful when a new version of the SSL VPN software is released. The new template file supplied with the software

can be exported and merged with a previously translated language file, so that only new and changed text strings need to be translated.

The next step is to import the language definition file your have translated to the VPN Gateway.

Import Language Definition File

1. In the System tree view, expand **Administration**.
2. Select **Operation**.

   The Host(s) screen appears.
3. Select **Language**.

   The Language form appears. Scroll down to Import/Export Language definition.

4. In the **Protocol** list box, specify the desired file transfer method.
5. In the **Server** field, enter the IP address of the file server from which you want to import the language definition file.
6. In the **File** field, enter the name of the translated language definition file, for example **`template.po`** .
7. In the **Language Code** list box, select the ISO 639 language code corresponding to your new language version.

   The language code is saved to the configuration together with the imported language definition file.

   Tip: To view valid language codes, click the Valid Languages button on top of the form. To limit the list to language codes starting with a specific letter, enter for example **e** in the Prefix field before clicking the button.
8. If required, enter the desired credentials for FTP import in the FTP User and FTP Password fields.
9. Click **Import Language**.

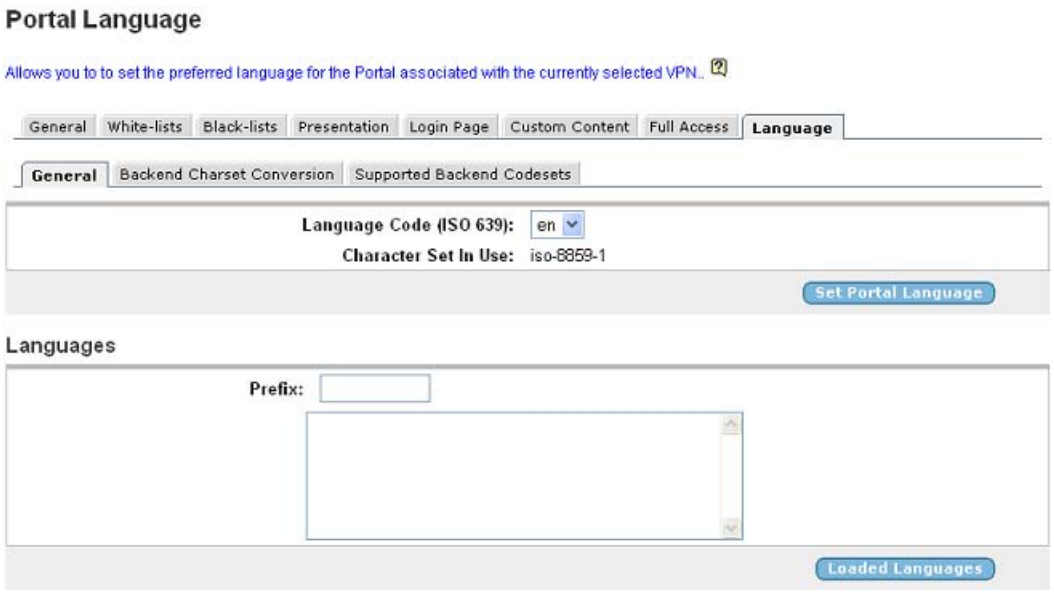
   The next step is to configure the Portal to use the new language version.

Configure the Portal to Use New Language

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
3. Select the portal from the settings.
4. Select **Language**.

   The Portal Language form appears.



5. In the **Language Code** list box, select the language code corresponding to the imported language definition file.
6. Click **Set Portal Language**.
7. Apply the changes.

   Connect to the Portal to view the new language version.

Backend Conversion

The Backend Conversion form is used to handle conversion of character sets for specified FTP file servers or SMB (Windows file share) file servers without Unicode capability.

Example: An FTP file server uses the ISO-8859-1 character set. The remote user browses to the Portal, connects to the FTP server on the Files tab and tries to display the file list. The VPN's existing character set is SHIFT_JIS (used for Japanese). This mismatch between character sets may cause characters in file names to not display correctly. To solve this, you

can configure the AVG to convert the ISO-8859-1 character set to the existing character set for the VPN (that is SHIFT_JIS) before sending the file list to the browser.

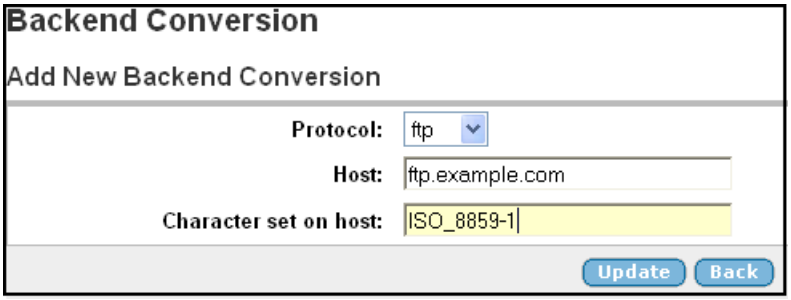
Character set conversion is not required for SMB servers running on Windows 2000 or XP, because they support Unicode natively.

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
3. Select the portal from the settings.
4. Select **Language**.

   The Portal Language form appears.
5. Select **Backend charset Conversion**.
6. Click **Add**.

   The Add New Backend Conversion form appears.



7. In the **Protocol** list box, select the desired protocol.

   This is to determine whether to make the conversion for an FTP file server or an SMB (Windows file share) file server.
8. In the **Host** field, specify the backend file server's host name or IP address.
9. In the **Character set on host** field, specify the character set to be converted, for example ISO-8859-1.
10. Click **Update** and apply the changes.
11. To add another backend conversion entry, repeat step 6 on page 213 to step 10 on page 213.

Upload Custom Content

The Custom Content feature is used to upload custom content (for example Java applets, HTML pages, executables) to an area on the VPN Portal.

To access uploaded content, the user should specify the whole path to the content, for example `https://vpn.example.com/content/example.html`. You can also create a Portal link

to the content, using the External Website link type (see Group Links on page 127). For a usage example, see Appendix I, "Using the Port Forwarder API" in the *User's Guide*.

Note:

Content uploaded to the Custom Content area is accessible without the user having to log on to the Portal.

1. Create a zip file containing the content you wish to upload.

   If the content you wish to import to the Portal requires caching on the remote user's machine when executed, create a directory called `Avaya_cacheable`. Then store the content in this directory before zipping the files (sub-directories may exist). Note that file and directory names are case sensitive.

   Examples of zip file contents:

   - noncacheable_content1.html
   - subdir/noncacheable_content2.html
   - avaya_cacheable/mycacheable_content1.html
   - avaya_cacheable/subdir/mycacheable_content2.html

   Also see the `/cfg/vpn/server/http/allow*` commands in the Command Reference used to allow or deny caching of different file types.

   Note:

   A previously imported zip file will be replaced with the new file. If you want to save existing Portal content, first export this content using the Export Custom Content button.

2. In the System tree view, select **VPN Gateways**.
3. Select the VPN name from the **Name** list.

   The VPN Summary screen appears.
4. Under **Settings**, select **Portal**.
5. Select **Custom Content**.

   The Portal Custom Content form appears.
6. In the **Protocol** list box, select the desired transfer protocol.
7. In the **Server** field, specify the IP address or host name of the file server where the zip file is stored.
8. In the **File** field, enter the name of the zip file that you wish to import to the Portal.
9. If needed, enter the credentials required for FTP transfer in the **User** and **Password** fields.

10. Click **Import Custom Content**.
11. In the **Access to Custom Content** list box, select **enabled** .

    This will make it possible for the remote user to access the custom content you have just uploaded.

Chapter 12: Configure Avaya Endpoint Access Control Agent

This chapter describes how to configure the Avaya VPN Gateway for use with Avaya Endpoint Access Control Agent (previously known as Tunnel Guard). Avaya Endpoint Access Control Agent (EACA) is an application that checks if the required components (executables, DLLs, configuration files) are installed and active on the remote user's machine.

How is Avaya Endpoint Access Control Agent Activated?

For HTTPS connections, the EACAapplet is downloaded to the client machine and started as soon as the user has successfully logged in to the Portal.

For Avaya VPN client, the EACAagent (if installed) is activated when the remote user logs in to the VPN.

Avaya Endpoint Access Control Agent SRS Rules

Which components to look for on the client machine is configurable through a certain specification, a Software Requirement Set (SRS) rule. The SRS rule in its turn should be mapped to one or more user groups, under **VPN Gateways>VPN Summary>EACA>SRS Rules**.

When EACA is done checking the client machine, it reports the result to the server. If the SRS rule check succeeded (required components were present on the client machine), the user is permitted access to intranet resources as specified in the user group's access rules. If the check failed, the behaviour is configurable. Either the session/tunnel can be torn down or the user may be granted restricted access.

If needed, a specific EACA SRS rule administrator can be created. The SRS rule administrator is only granted access to the EACA applet. Contact your ISP if you wish to enable a specific SRS rule administrator with limited access.

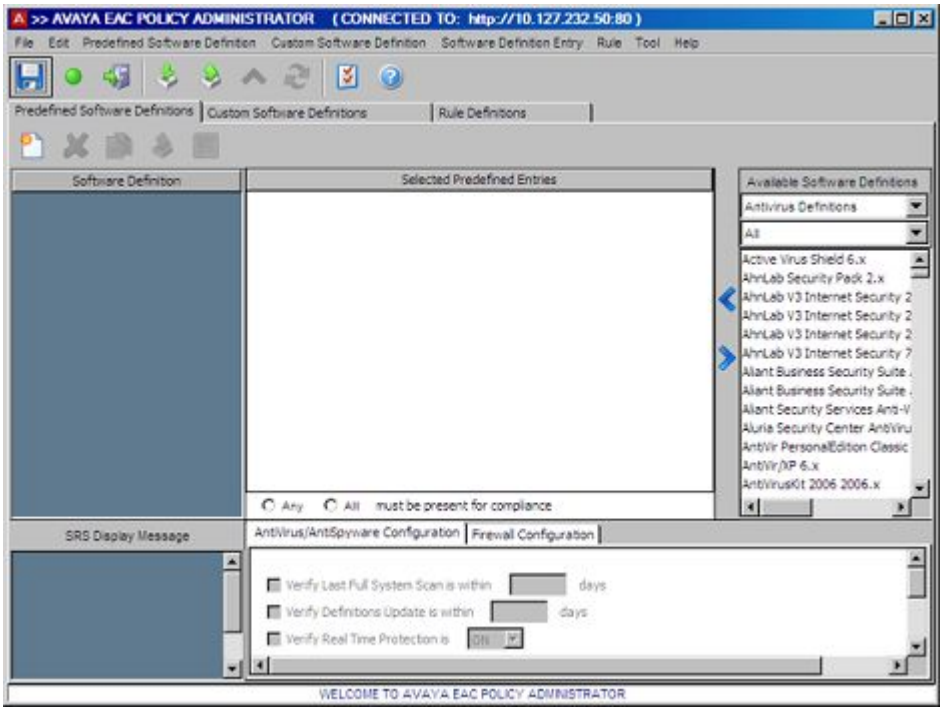
Configure SRS Rules

To configure EACA SRS rules, log in to the Browser-Based Management Interface (BBI).

Launch the Avaya Endpoint Access Control Agent Applet

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN Gateway name.
3. Under **Settings**, select **EACA**.
4. Select **SRS Rules**.
5. Click **Launch**.

   The EACA applet used for configuring SRS rules is displayed.



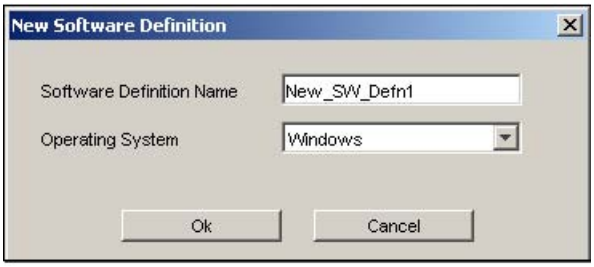
The EACA applet has several buttons with varied functions. Refer to the “Configure Avaya Endpoint Access Control Agent” chapter in the BBI Application Guide for more information about these buttons.

Create New Predefined Software Definitions

Predefined SRS Entry defines the set of AntiVirus, AntiSpyware, and Firewall vendors, attributes like Last virus update, Firewall is on/off so on. Start by creating a software definition.

1. Click on the **Predefined Software Definitions** tab.
2. Select **New Definition**. You can select the New Definition by using the following methods:
   - From **Predefined Software Definition** Menu.
   - Click **New Definition** button.

   The New SRS window appears.



3. Enter a name for the software definition and Operating System.

   For example, to create a software definition specifying the antivirus software modules that must be present on the client system, enter the name Antivirus. The new software definition is added in the Software Definition area top left.
4. Click **OK**.

Adding a vendor

Follow these steps to add vendor(s) to a predefined software definition:

1. Select the name of the predefined software definition entry for which you want to map the vendor.
2. Select the name of the available software definition entries (vendor) from right side of the pane.
3. Click on the **<** to map the available software definition entries to the predefined software..
4. Select the following options for EACA rule validation:
   - Any - Any of the predefined entries are validated.

- All - All of the predefined entries are validated.

5. Specify the AntiVirus\Antispyware Configuration and Firewall Configuration parameters of the selected entry.

Note:

Depending upon the entry selected, the parameters of the antivirus/antispyware or firewall configurations differs.

6. Click **Apply**.
7. Click **Save** to save the defined entries.

Note:

Percentage of the SRS data being saved is displayed at the bottom of the screen.

Import/Export files

You can do the following by using the import/export options:

- Select multiple Software Definitions by clicking export to export selected entries.
- Select multiple rules.
- Export all Rules and definitions by a single click.
- Import older versions of definitions.

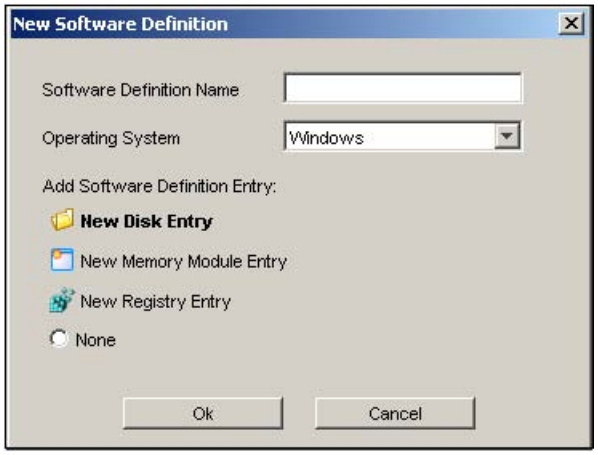
Note:

If there are any duplicates while importing warnings are provided to either overwrite or keep the existing entries or to cancel the operation

Create a New Custom Software Definition

Custom SRS Entry defines set of software elements like files, processes, modules, registry and so on. That must exist on compliant desktop. Follow these steps to create a new custom definition:

1. Click on the **Custom Software Definitions** tab.
2. Select **New Definition**. You can select the New Definition by using the following methods:
   - From Custom Software Definition Menu.
   - Click New Definition button.



3. Enter the name of the software definition.
4. Select the Operating System for the software definition.
5. To add a software definition entry, select the following options depending upon what you want as a new entry:
    - New Disk Entry
    - New Memory Module Entry
    - New Registry Entry
    - None
6. Click **OK**.

Add Entries to Software Definition

There are different ways of specifying which files, software executables and so on that should be (or should not be) present/running on the client system:

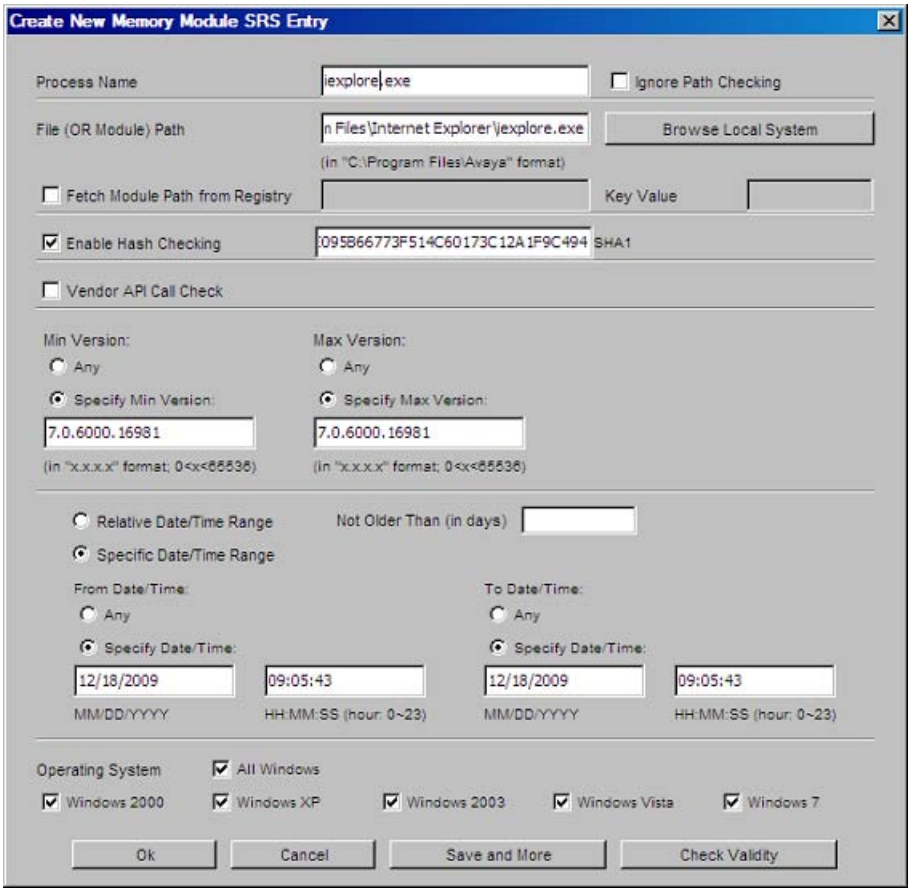
- Specify the path to the file without having to run the process yourself
- Select the desired modules from the processes that are running on your admin PC

Add New Memory Module Entry

Follow these steps to add new memory module entry:

1. Click on the **Custom Software Definitions** tab.
2. Select **New Memory Module Entry**. You can invoke the New Memory module by using the following methods:
    - From Software Definition Entry menu
    - From New Software Definition screen in Custom software Definition.

• Right click on the software definition entry at the left side of the window.



3. In the **File (OR Module) Path** field, verify that the correct file or module is selected.

   If you want to add another file or module to the current software definition, click **Browse Local System** and find the desired file.

4. Select the **Fetch Module Path from Registry Entry** check box, if the file's registry entry should be checked rather than the executable itself.

   Then enter the desired path and key value in the fields. A registry check provides an easier way to validate applications and to check for patch levels.

5. To ignore path checking, select the **Ignore Path Checking** check box.

   If enabled, the client system will be searched for the specified file name, irrespective of path to folder.

6. In the **Process Name** field, enter the name of the process whose module you wish to add as a software definition entry.

   The name of the selected process is displayed by default.

7. In the Min and Max Version area, you can specify the minimum or maximum version of the file/module.

   If there are no restrictions as to version (minimum or maximum) select Any.

8. Select the **Relative Date/Time Range** button and specify the maximum file age.

   Lets you specify the file age in number of days.

   OR

9. Select the **Specific Date/Time Range** button and specify the desired time range or specific date/time.

   Lets you specify a date/time range or an exact date/time referring to when the file was created or last modified.

10. Select the **Vendor API Call Check** check box to implement a 3rd-party API call for doing additional checking on the software.

    One of the features of Avaya Endpoint Access Control Agent is the ability to specify an API that you want to use to check a file, such as an executable. Avaya Endpoint Access Control Agent supports the use of API calls that check on either startup, when the component (for example, an executable or DLL) is launched from a file on disk; or during runtime, when a component is already launched and running in memory.

11. Select the **Enable Hash Checking** check box to enable hash value checking of the current SRS entry.

    Then paste the hash value to be checked in the **Hash Value** field. The hash value of a selected file/module (if any) is displayed by default.

12. Click **OK**.

    The file/module is added as an entry in the selected software definition. By clicking the **Save** and **More** button, the entry is saved but the Create New Memory Module SRS window remains open so you can add more entries to the current software definition.

13. Specify the operating system based on which SRS entry is created.

14. Click **Check validity** button to check for dynamic value of complete path with all variables parsed to their values on local PC.

Select Modules/Files From Running Processes

Follow these steps to select the desired modules from the processes that are running on your admin PC:

1. Click on the **Custom Software Definition** tab.
2. Click on memory snapshot button on the menu.

Note:

The custom software definition entry should be created for memory snapshot to be active.

All processes that are currently running on your local PC system are displayed at the bottom of the pane.

3. Select a process or application, all its associated modules are listed to the right.
4. Double click on the associated module.
5. Click **OK**.

   The module is included in the entry.

Add File on Disk

This method lets you add files that are not shown in the memory snapshot. Select a file from the local file system, for example a text configuration file, and add it as a software definition entry. You can also add files that are not present on your file system, for example malicious files. Using the NOT operand when forming logical expressions, you can then instruct EACA to verify that certain files are not present on the client system.

1. Click on the **Custom Software Definitions** tab.

   The New SRS window appears.
2. Select **New Disk Entry**. You can invoke the new disk by using the following methods:

   - From Software Definition Entry menu.
   - From New Software Definition screen in Custom software Definition.
   - Right Clicking on the Software definition entry at the left side of the window.

   The New Disk Entry window is displayed.
3. In the **File (OR Module) Path** field, enter the path to the file.

   To add a file that exists on your system, click the **Browse Local System** button and find the desired file.
4. Select the **Fetch Module Path** from **Registry Entry** check box, if the file's registry entry should be checked rather than the executable itself.

   To add a file that exists on your system, click the **Browse Local System** button and find the desired file.
5. Then enter the desired path and key value in the fields.

   A registry check provides an easier way to validate applications and to check for patch levels.

6. Specify the desired limitations regarding version and file age.

   See the previous section for more detailed information about these options.

7. Select the **Enable Hash Checking** check box to enable hash value checking of the current SRS entry.

   Then paste the hash value to be checked in the **Hash Value** field. The hash value of a selected file/module (if any) is displayed by default.

8. Specify the operating system based on which SRS entry is created.
9. Click **Check validity** button to check for dynamic value of complete path with all variables parsed to their values on local PC.
10. Click **OK**.

The file/module is added as an entry in the selected software definition. By clicking the **Save** and **More** button, the entry is saved but the Create New On Disk SRS Entry window remains open so you can add more entries to the current software definition. The file is added as a software definition entry on the right pane.

Add New Registry Entry

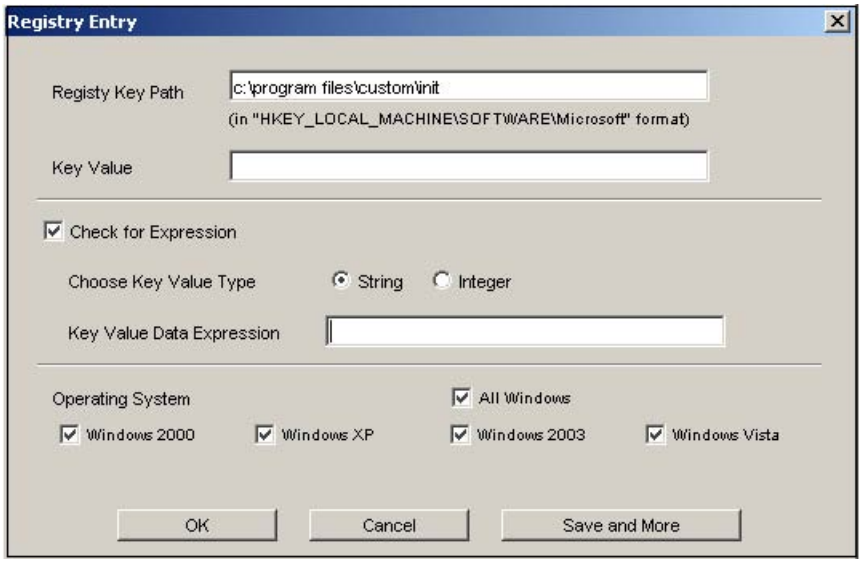
Follow these steps to add a new registry entry:

1. Click on the **Custom Software Definitions** tab.
2. Select **New Registry Disk Entry**. You can invoke the New Registry by using the following methods:

   • From Software Definition Entry menu.

   • From New Software Definition screen in Custom software Definition.

   • Right Clicking on the Software definition entry at the left side of the window.



3. Enter the path where Registry key is placed.
4. Enter the key value.

Note:

A registry check provides an easier way to validate applications and to check for patch levels.

5. Choose the key type value. It can be string or integer value.
6. Enter the key value expression.
7. Select the operating system which supports the rule.
8. Select the operating system which supports the rule.

Create Logical Expressions

To be able to specify an SRS rule that comprises a number of different requirements, you can create a logical expression. The logical expression should contain the conditions that must be true for the Avaya Endpoint Access Control Agent (EACA) checks to pass. For example, a logical expression can define several applications that must be present on the client computer or that either of two applications must be present.

Having created a logical expression with the desired conditions, simply select the expression for the EACA SRS rule.

1. Create the desired software definitions.

For example, you may create one software definition identifying an antivirus program, another software definition that identifies a certain executable, a third that identifies a certain dll file and so on.

2. Click on **Rule Definitions** tab.

   EACA rules and expressions with the same names as the software definitions have been created and appear on the **Rule Definitions** tab.

   Two EACA rules have now been created, each defining a unique application. To create one EACA rule comprising both applications, we should start by creating a new logical expression.

3. Select the desired expression in the Available expressions area and click the **>** button.

   The expression is copied to the right area.

4. Select another expression that you will use to form a new logical expression in combination with the first.

5. Using the radio buttons, select the type of expression you wish to construct, in this example an AND expression.

   The AND operation lets you construct a logical expression where both conditions must be met for the EACA checks to pass. The OR operation lets you construct an expression where either of the conditions must be met for the EACA checks to pass. The NOT operation lets you construct an expression where the condition must not be met for the EACA checks to pass, for example the file or files in the software definition must not be found on the client machine.

6. Click on **Form EAC Rule Expression**.

   A new expression is created and copied to the Available Expressions area.

7. To create an EAC rule, click on **Rules Definitions** tab. You can create a rule by using the following methods:

   - From EAC Rule menu, select **New EAC Rule**.
   - Click on **New EAC Rule** button.

8. Enter a name for the EAC rule and click **OK**.

   The new rule name appears in the EAC Agent Rule Name column.

9. In the EAC Rule Expression column, select the expression you have created.

   Any logical expression that you create may be used in a new logical expression, for example to construct more complex conditions.

General

Add Avaya Endpoint Access Control Agent Rule Message

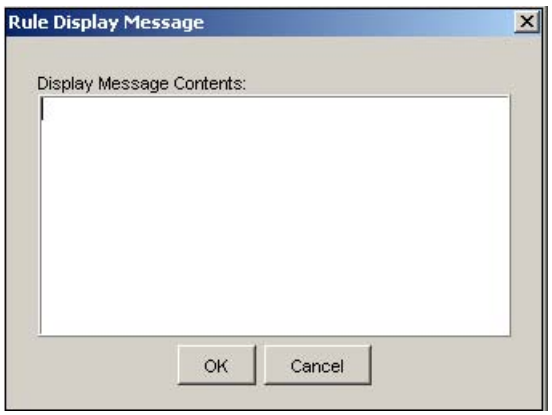
By adding an EACA rule message to an EACA rule, you can provide important information to the user, for example the reason why the EACA checks failed and/or the recommended action. This information is expanded by the <*var:tgFailureReason*> variable, along with the EACA rule expression name. The variable can for example be included in a linkset text. If teardown mode is used, the comment is automatically displayed on the Portal Login page (see Restricted Mode vs. Teardown Mode on page 240).

1. Click on the **Rule Definitions** tab.
2. In the **Display Message on Failure** tab, click the row corresponding to the SRS rule for which you wish to add a comment.

   The following button appears:

3. Click the button to display the Rule Display Message.

4. Type the message and click **OK**.

   The message is displayed at the left side of the screen.

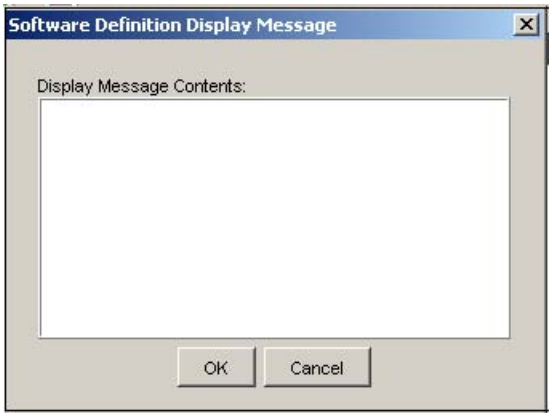
Add Software Definition Message

The software definition message is shown in the message displayed when the user clicks the **details** link on the Portal login page (see Restricted Mode vs. Teardown Mode on page 240). It is also included in the <*var:tgFailureDetail*> variable. The variable can for example be included in a linkset text to print the result of an EACA check that has failed. The variable

expands to the software definition comment and detailed information about missing/present files on the client machine.

1. Click on **Predefined Software Definitions** tab.
2. Select **Predefined Software Definition** menu.

   The Software Definition Display Message window is displayed.



3. Type in the desired text and click **OK**.

Add Custom Software Definition Message

Follow these steps to add a message to custom software definition:

1. Click on **Custom Software Definitions** tab.
2. Click the **New Software Definition** icon.

   The New Software Definition window is displayed.
3. Type in the desired text and click **OK**.

Delete a Predefined Software Definition

Follow these steps to delete a predefined software definition:

1. Click on **Predefined Software Definitions** tab.
2. In the **Software Definition** column, select the desired software definition.
3. On the **Predefined Software Definition** menu, select **Delete Definition**.

   Note that you cannot delete a software definition that is used in an EACA rule. Delete the EACA rule first.

Delete a Custom Software Definition

Follow these steps to delete a predefined software definition:

1. Click on **Custom Software Definitions** tab.
2. In the **Software Definition** column, select the desired software definition.
3. On the **Predefined Software Definition** menu, select **Delete Definition**.

   Note that you cannot delete a software definition that is used in an EACA rule. Delete the EACA rule first.

Delete a Avaya Endpoint Access Control Agent Rule

Follow these steps to delete an EACA rule:

1. Click on the **Rule Definitions** tab.
2. In the **Rule** table, select the desired rule.
3. Under menu, select the **EACA Rule** option.
4. Click on **Delete EACA Rule** option under it.
5. Click **Yes**.

Delete an Expression

Follow these steps to delete a software definition:

1. Click the **Rule Definitions** tab.
2. In the Available Expressions area, select the desired expression and click the **Delete Expression** button.

   Note:

   You cannot delete an expression that is used in an EACA rule.

Set Avaya Endpoint Access Control Agent Preferences

Follow these steps to set the preferences for the Avaya Endpoint Access Control Agent:

1. Under menu, click **Preferences**.

Configuration Settings screen appears.

2. Select Look and Feel of the applet. You can select following options:
   - native
   - cross platform
3. Select the color scheme for the applet. You can select the following colors:
   - red
   - green
   - orange
   - Teal
   - blue
4. Select the default hash algorithm.
5. Set the icon size.
6. Check the **Connect At Startup** box and specify the protocol, IP address, and port number required to start the Avaya Endpoint Access Control Agent.
7. Check the box **AutoGenerate Avaya Endpoint Access Control Agent Rule** box to generate the Avaya Endpoint Access Control Agent Rule automatically.
8. Check **Run Memory snapshot At Start Up** to run the snapshot during the startup of the Avaya Endpoint Access Control Agent applet.
9. Check the **Set Current Size As Default** if you want to retain the current size of the applet as the default size.
10. Click **OK** to apply the preferences.

Note:

You need to restart the Avaya Endpoint Access Control Agent applet for the changes to get affected.

Set Contivity for Avaya Endpoint Access Control Agent

You can connect the EACA to any AVG box by changing its configuration settings. Follow these steps to set the new connection for the EACA:

1. Under menu, click on **Connect To**.
2. Specify the connection profile name.
3. Specify the protocol. It can be http or https.
4. Specify a valid host address.e.g: `10.127.232.41`

5. Specify the port number.
6. Click **Create**.

Making API Calls

Avaya Endpoint Access Control Agent requires a Windows Platform DLL that implements at least one common entry point as described.

Windows

```
#include <windows.h>
/* return values */
#define STATUS_SUCCESS 0
#define STATUS_FAILURE -1
#define STATUS_REQUIRES_UPDATE 1
/* simple check */
int WINAPI CheckStatus(void);
```

This API would block until it returns one of the required statuses in 10 seconds or less. If an answer is not returned in a timely manner, it is assumed the personal firewall software is unavailable, and the call times out and returns an error message.

Configure Avaya Endpoint Access Control Agent

This section includes an example of how to set up a working EACA solution. It illustrates how to configureEACA to check that the proper anti-virus program is installed on the remote user's machine and – if the EACA checks fail – how to direct the remote user to a web site where he can update his virus program.

Enable Avaya Endpoint Access Control Agent

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN Gateway name.
3. Under **Settings**, select **EACA**.
4. Select **Setup**.

   The EAC Agent Setup form appears.
5. In the **Status** list box, select **enabled.**

6. In the **Fail Action** list box, set the desired fail action.

   By setting the action to teardown, the tunnel will be torn down if the EAC Agent checks fail. By setting the action to restricted, the remote user can be given limited access if the EAC Agent checks fail. In this example we will set the fail action to restricted.

7. In the **Recheck Interval** field, set the desired time interval for SRS rule rechecks.

   This step sets the time interval for SRS rule rechecks made by EAC Agent on the client machine. If a recheck fails (that is the required file is no longer present or the required process is no longer running), the tunnel/session is terminated. Depending on access method, this means that the remote user is kicked out from the Portal or has his IPsec tunnel torn down.

8. In the **Log Level** list box, select the desired log level (optional).

   This step sets the log level for debugging information from the Avaya Endpoint Access Control Agent applet. The information is displayed in the remote user's Java Console window and can be used to track errors in EAC Agent SRS rules.

9. In the **Display SRS Failure Details** list box, select the desired option.

   This step lets you specify whether or not EAC Agent SRS rule failure details should be displayed to the user.

   - **on:** The **details** link is displayed on the Portal login page if the EAC Agent checks fail and **Fail Action** (see preceding step) is set to teardown. When the user clicks the **details** link, more detailed information about the cause of the failure is displayed in a separate window. The on setting also enables printing the failure details in a linkset text, using the <*var:tgFailureDetail*> variable. See Add Software Definition Message on page 228 for more information.
   - **off:** The **details** link is not displayed. The <*var:tgFailureDetail*> variable is not expanded.

   Note:

   This setting has no impact on the behaviour of the installed EAC agent, that is even if the setting is disabled on the AVG, it might be enabled in the EAC agent settings.

10. Click **Update** and apply the changes.

Avaya Endpoint Access Control Agent Settings

The EACagent is started (if enabled) when the remote user connects to the VPN with the IPsec VPN client (formerly the Contivity VPN client). Following are instructions on how to configure the AVG for use with the EAC agent.

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN Gateway name.
3. Under **Settings**, select the **EACA**.

4. Select **Agent**.

   The EAC Agent form appears.

5. In the **Agent Query Timeout Interval** field, specify the interval between connection attempts.

   This step lets you specify the interval between connection attempts from the EAC server (on the VPN Gateway) to the EAC client (on the client machine). This setting only applies to clients with the EACAagent installed – not the EACAapplet downloaded from the Portal.

6. In the **Agent Minimum Version** field, specify the minimum version of the EAC application (agent).

   This step lets you enter the minimum version of the EAC application. A VPN client with an older version of the EAC agent will not be able to connect to the VPN Gateway. This setting only applies to clients with the EAC agent installed – not the EAC applet downloaded from the Portal. The default value is 0.0.0.0, that is all client versions are allowed.

7. Click **Update** and apply the changes.

Configure Linksets

Typically, linksets are configured to contain a set of links. In this example we will use the linksets used to communicate information to the remote user on the Portal.

First, we will define a linkset to print the result of the EAC checks when they succeed.

1. In the System tree view, select **VPN Gateways**.
2. Select the VPN Gateway name.
3. Under **Settings**, select **Link Sets**.
4. Click **Add**.

   The Add New Linkset form appears.

5. In the **Name** field, enter a name for the linkset.

   In this example we will call the linkset tg_passed.

6. In the **Text** field, enter the linkset text.

   The linkset text should read `"The EAC checks succeeded!".`

   Typically, the linkset text creates the heading for a set of links. In this example, we will simply use it to print the result of the EAC checks. No links will be configured for this linkset.

7. Click **Update**.
8. Click **Add** to define a new linkset.

This linkset should print the result of the EAC checks when they fail.

9. In the **Name** field, enter the name `tg_failed`.
10. In the **Text** field, enter the linkset text.

    The linkset text should read `"The EAC checks failed. Click the link below to download new anti-virus software. "`.
11. Click **Update**.

Configure a Link

The tg_failed linkset should also contain a link to a web site where a new anti-virus program can be downloaded.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.
3. Under **Settings**, select **Link Sets**.
4. In the **Portal Linkset** list box, select the portal linkset where the link should be included (that is **tg_failed**).
5. Click **Refresh**.
6. Click **Add**.

   The Add Portal Links form appears.
7. In the **Text** field, enter the link text to appear on the Portal's Home tab.

   The link text should read "Anti-virus program download site".
8. In the **Link Type** list box, select **Internal Website** as link type.
9. Click **Continue**.

   The form is expanded.
10. Under **Internal Link Settings**, in the Protocol list box, select **http**.
11. In the **Host** field, enter the address of the anti-virus program download site, for example **`antivirus.example.com.`**
12. In the **Path** field, enter a forward slash to imply the web server's root or specify the desired path, for example `/update/file.html.`
13. Click **Update**.

Configure a Network

This section describes how to create a network definition identifying a web server on the intranet. This is the web site where the remote user will be able to download the anti-virus program.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.
3. Under Settings, select **Authorization**.
4. Select **Networks**.

   The Networks form appears.
5. Click **Add**.

   The Add Network form appears.
6. In the Name field, enter a name for the network, for example anti-virusweb.
7. Click **Continue**.

   The form is expanded.
8. Under Network Subnets, click **Add**.

   The Add Network Subnet form appears.
9. In the Hostname field, enter the host name of the anti-virus program download site.

   When creating a subnet, enter either the host name or the network address/ netmask.
10. Click **Add**.
11. Apply the changes.

Configure a Group

In this example we will choose the **novice** user type for the group. This will limit display to the **Home** and **Tools** tabs when the EAC checks fail. In addition, no access rules will be created for the group's base profile, that is the parameters specified directly on group level. This will deny access to all networks, services and paths. Instead, we will use extended profiles to specify the group's access rights, depending on whether the EAC checks fail or succeed.

The reason for not specifying access rules on group level is that the access rules pertaining to the group's base profile are appended to those of the extended profile.

You can read more about groups, access rules and profiles in Groups, Access Rules and Profiles on page 35.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.
3. Under **Settings**, select **Groups**.
4. Click **Add**.

   The Add New Group form appears.
5. In the **Name** field, enter a name for the group, for example **staff**.
6. In the **User Type** list box, select **novice**.
7. Click **Update**.
8. In the System tree view, select **VPN Gateways**.
9. Select the name of the VPN Gateway.
10. Under **Settings**, select **EACA**.
11. Click on **SRS Rules** tab.
12. To configure SRS Rules click the **Launch** button.

Configure Client Filters and Extended Profiles

Two client filters need to be created. The first client filter should be triggered when the EAC checks succeed. The other client filter should be triggered when the EAC checks fail.

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway.
3. Under settings, select **Groups**.
4. Select the Group name.
5. Select **Extended Profiles**.

   Extended Profiles form appears.
6. Click on **Add Profile**.

   Client filters and extended profiles are automatically added to the table.
7. If you want to view only the client information, then click on **End Point Filter** link.
8. If you want to view only the extended profile information, then click on **Extended Profiles** button in Client Filters screen.

Configure Access Rules

1. In the system tree view, select **VPN Gateways**.

   VPN Gateways form appears.
2. Select the name of the VPN Gateway.
3. Under settings, select **Groups**.
4. Select the Group name.
5. Select **Extended Profiles**.

   Extended Profiles form appears.
6. Click on **Add Profile** button.

   Client filters and extended profiles are automatically added to the table.
7. Under Actions column in the table, click on the modify link.
8. Click on **Access Lists** tab.
9. Click **Add**.

   The Add Rule form appears.
10. Keep the asterisks (*) in the Network, Service and Application list boxes. This implies all networks, port numbers, protocols and paths.
11. In the Action list box, select **Accept**.
12. Click **Update**.

Map Linksets to Extended Profiles

1. In the system tree view, select **VPN Gateways**.

   VPN Gateways form appears.
2. Select the name of the VPN Gateway.
3. Under **settings**, select **Groups**.
4. Select the Group name.
5. Select **Extended Profiles**.

   Extended Profiles form appears.
6. Click on **Add Profile** button.

   Client filters and extended profiles are automatically added to the table.
7. Under **Actions** column in the table, click on the modify link.

8. Click on **Linksets** tab.

   Extended Linksets form appears.

9. In the **Portal Linksets** list box, select the linkset **baselinks**.

   This linkset also contains a link that directs the remote user to the anti-virus program download site.

10. Click **Add**.

    This maps the linkset tg_failed to the extended profile tg_failed.

11. Apply the changes.

    For more instructions on how to create groups, access rules and profiles, see Configure Linksets on page 234.

Test the Example Configuration

To test how EAC behaves when configured as described in the previous example, proceed as follows:

1. In your browser, enter the IP address or domain name of the desired VPN.

   The Portal login page appears.

2. Log in to the Portal.

   This example assumes that you have configured a user that belongs to the staff group. For instructions on how to add users to the local database, see Authentication Methods on page 75.

   The EACA applet is downloaded to your machine. Because the user is a member of the staff group, and the SRS rule is mapped to this group, the EACA applet will now check if the requested anti-virus program is present on the user's PC.

   In this example, we have used the wizard to set restricted mode as fail action. This means that the tunnel is not torn down even if the EACA checks fail. The result is displayed on the Portal page.

Avaya Endpoint Access Control Agent Checks Succeeded

The “EACA checks succeeded!” message appears if the requested anti-virus software is present on the client PC.

To confirm that EACA is running and that the checks have succeeded, the EACA Success icon is displayed to the right of the Portal tabs (for an explanation of the other icons, see The Portal from an End-User Perspective on page 287).

The client filter called tg_passed triggered when the EACA checks succeeded. This in its turn triggered Extended profile 1 (tg_passed) in the staff group, because Extended profile 1 references the client filter tg_passed.

The linkset used in Extended profile 1 is a linkset called tg_passed. It has no links but prints the text "The EACA checks succeeded!".

Extended profile 1 gives access to all networks and services. It is configured with the user type advanced, which gives access to all Portal tabs.

Avaya Endpoint Access Control Agent Checks Failed

The “EACA checks failed” message appears if the requested anti-virus software is not present on the client machine.

To confirm that EACA is running but the checks have failed, the EACA Failure icon is displayed to the right of the Portal tabs (for an explanation of the other icons, see The Portal from an End-User Perspective on page 287).

The client filter called tg_failed triggered when the EACA checks failed. This in its turn triggered Extended profile 2 (tg_failed) in the staff group, because Extended profile 2 references the client filter tg_failed.

The linkset used in Extended profile 2 is a linkset called tg_failed. It prints the text "The EACA checks failed. Click the link below to download new anti-virus software". The linkset includes one link, directing the user to an anti-virus program download site.

Extended profile 2 only allows access to the download site. It is configured with the user type novice, which gives access to the **Home** and **Tools** tabs only.

Restricted Mode vs. Teardown Mode

The previous example shows the result when EACA operates in restricted mode. The user is logged in to the Portal but access is restricted.

If EACA had been set to operate in teardown mode, the user would not have been logged in to the Portal at all. Instead, the Login page displays the result of the EACA check.

The EACA rule expression (srs-test) and the EACA rule comment (This is a Test Rule) are automatically displayed. For a description of how to configure the desired EACA rule comment, see the section General on page 228.

When the user clicks the **details** link, a message window appears.

This window provides more detailed information about the failed EACA check, for example a specification of missing files on the client machine. The text that reads "To be used for testing" in the preceding example is configurable. See the section Add Software Definition Message on page 228.

If desired, the **details** link can be hidden. Go to **VPN Gateways>EACA>Setup** and select **off** in the **Display SRS Failure Details** check box. This will also disable the *<var:tgFailureDetail>* variable.

Using predefined software definition entries

Using predefined set of software entries you can administer the software definition with minimal effort. To use these predefined software entries follow these steps:

1. Launch EACA administration user interface either directly or through SREM application.

   EACA window with 3 tabs is displayed:

   - Software Definition
   - EACA Rule
   - Predefined Software Definition Entries

2. Click **Predefined Software Definition Entries**.

   List of all predefined software supported by OPSWAT, PatchLink or other third party vendors can be viewed.

3. Select the version number.
4. Click **Add**.
5. Select another version number.
6. Click **Add**.
7. Select one of the following options:

   - All – Indicates, that all are required to be present on desktop PC.
   - Any – Indicates, that any one of the applications needs to be present on desktop PC.

8. Click **Create Software Definition**..
9. Add a comment message for each entry
10. Customize the entry to check for definition file/engine version.
11. Configure action to run if policy fails based on the type of entry.

Chapter 13: WholeSecurity

Symantec WholeSecurity Confidence Online offers on-demand protection for all users logging into the network through remote access technologies, like SSL VPNs.

How Does it Work?

When the remote user connects to the VPN, he or she is automatically redirected to a WholeSecurity Confidence Online server on the intranet. The Confidence Online software is downloaded to the endpoint machine and performs a scan to identify any eavesdropping threats, including Trojan horses, remote controls, keystroke loggers and worms – before the user has actually logged on to the VPN.

If no threat is found, the VPN's login screen appears. If malicious code is detected, the offending process can be terminated, quarantined and reported.

Configuration

The configuration on the Avaya VPN Gateway (AVG) is limited to enabling WholeSecurity, specifying the URL to a WholeSecurity Confidence Online server and configuring a user access group that allows redirection to an intranet web site prior to logging in to the VPN.

The rest of the configuration is done using the WholeSecurity Confidence Online management interface. It includes specifying a deployment, which defines the type of scan to be performed and what action should be taken when the scan fails. For instructions, see the Confidence Online manual.

Requirements

The following requirements apply for a successful deployment:

- Fully qualified domain names (FQDNs) must be used to access the AVG and the WholeSecurity server. IP addresses do not work.
- The AVG should use a certificate that matches its FQDN. A certificate created by the wizard will not work.
- The client browser should trust the certification authority (CA) of the AVG certificate. If a private CA is used, that CA certificate should be added to the browser. The CA certificate

must be added to Internet Explorer (MSCAPI store) even when using Firefox/Mozilla. If a self-signed certificate is used, that certificate should be added to the browser as a "Trusted Root Certification Authority".

- The AVG and WholeSecurity servers should be in the same domain. For example, if the AVG is vpn.example.com, the WholeSecurity server should also reside in the example.com domain, e.g as ws.example.com.

Configure a Deployment

Before you start configuring the AVG, install the WholeSecurity Confidence Online software on a server on the intranet and configure a deployment. See the Confidence Online manual for instructions.

Note:

The WholeSecurity server creates a virtual directory named `/integration` and by default, access is denied to all IP addresses. Because the AVG needs to access scripts in this directory to check the scan results, you must add the AVG's interface IP address (not the Portal IP address) to the allowed list. This can be done using the IIS management console or equivalent.

Enable Whole Security

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. In the System tree view, select **VPN Gateways**.

   VPN Gateways form appears.
5. Select the name of the VPN Gateway.
6. Under settings, select **General**.
7. Select **WholeSecurity**.

   The WholeSecurity Settings form appears.
8. In the **Status** list box, select **on.**
9. In the Deployment URL field, specify the URL to the WholeSecurity Confidence Online server.

   This step lets you enter a URL to the WholeSecurity Confidence Online server, according to the following format:

`https://<confidence_online_server>/llclient /<deployment>/online.html.`

For example, if the Confidence Online server is running at `ws.example.com` and the deployment is called **SSLVPN**, the resulting URL can be:

`https://ws.example.com/llclient/SSLVPN/online.html`

10. In the **Redirect URL On Logoff** field, specify a logout URL.

    This is the page to which the user is directed when logging out from the VPN session. When WholeSecurity is enabled, the Login page will not be displayed on logout.

11. Click **Update** and apply the changes.

Configure a Network Definition

For the remote user to be subject to a Confidence Online scan before actually logging in to the VPN, redirection to the Confidence Online server must take place as soon as the remote user points to the URL of the VPN. Normally, the remote user cannot be redirected to a site on the intranet without first logging in to the VPN. However, by creating a network definition and an anonymous group, this will be allowed.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. Select **VPN Gateways**.

   VPN Gateways form appears.

5. Select the name of the VPN Gateway.
6. Under settings, select **Authorisation**.
7. Select **Networks**.

   The Networks form including previously configured networks is displayed.

   We will start by creating a network definition corresponding to the WholeSecurity Confidence Online server.

8. Click **Add**.

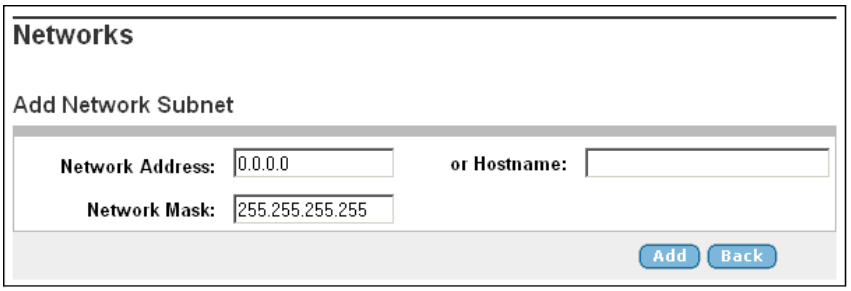
   The Add Network form appears.

9. In the **Name** field, enter a name for the network definition, for example WholeSecurity.
10. Click **Continue**.

    The form is expanded with the Network Subnet subform.

11. Click **Add** to add a new subnet.

    The Add Network Subnet form appears.



12. In the Hostname field, enter the name of the Confidence Online server.

    This could for example be **`ws.example.com.`**

13. Click **Add**.
14. Select **VPN Gateways**.

    VPN Gateways form appears.

15. Select the name of the VPN Gateway.
16. Under settings, select **Authorisation**.

    The network should now be added to the list of network definitions.

17. Apply the changes.

Configure an Appspec Definition

By specifying an application specific (appspec) definition identifying specific paths, you can limit the user's access rights on the WholeSecurity Confidence Online server.

This appspec definition should later be referenced in the anonymous group's access rules.

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. Select **VPN Gateways**.

   VPN Gateways form appears.

5. Select the name of the VPN Gateway.
6. Under settings, select **Authorisation**.
7. Select **Application**.

   The Application Specific Entries form appears.

8. Click **Add**.

   The Add Application Specific Entry form appears.

9. In the **Name** field, enter the name of the appspec entry, for example **`WholeSecurity`** .
10. Click **Update**.
11. Select **VPN Gateways**.

    The VPN Gateways form appears.

12. Select the name of the VPN Gateway.
13. Under settings, select **Authorization**.
14. Select **Applications**.

    The General form appears.

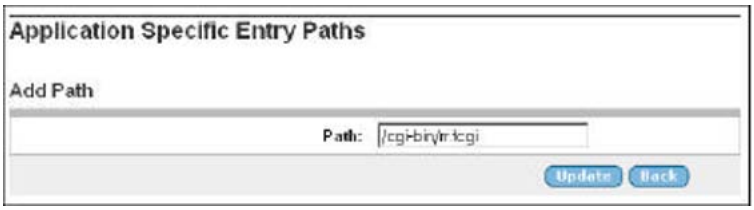
15. Go to **Application Entry Paths**.

    The Application Specific Entry Paths form appears.

16. Click **Add**.

    The Add Path form appears.

17. In the **Path** field, enter the first path, that is `/cgi-bin/rr.fcgi`.



18. Click **Update**.

    The path is added to the Application Specific Entry Paths form.

19. Click **Add** to add a second path.

    The Add Path form appears.

20. In the **Path** field, enter the second path, that is **`/llclient/ <deployment>`**.

    Replace <deployment> with the name of the deployment you have configured in the WholeSecurity Confidence Online software.

    The preceding example shows a path where the name of the deployment is SSLVPN.

21. Click **Update**.

    The Application Specific Entry Paths form is redisplayed with the second path added.

22. Apply the changes.

Configure an Anonymous Group

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Click **Config** tab.
4. Select **VPN Gateways**.

   VPN Gateways form appears.

5. Select the name of the VPN Gateway.
6. Under settings, select **Groups**.

   The Groups form appears.

7. Click **Add**.

   The Add New Group form appears.

8. In the **Name** field, enter a name for the group, for example **WholeSecurity** .
9. Click **Update**.

   The Groups form is redisplayed with the new group added to the list.

10. Under settings, select **Groups**.
11. Select **Access List**.

    The Firewall Access List form appears.

12. Click **Add**.

    The Add Rule form appears.

13. In the **Network** list box, select the network definition called **WholeSecurity** .

    This is the network definition we created in the section Configure a Network Definition on page 245. By referencing this network in the access rule, access will be granted to the Confidence Online server and nothing else.

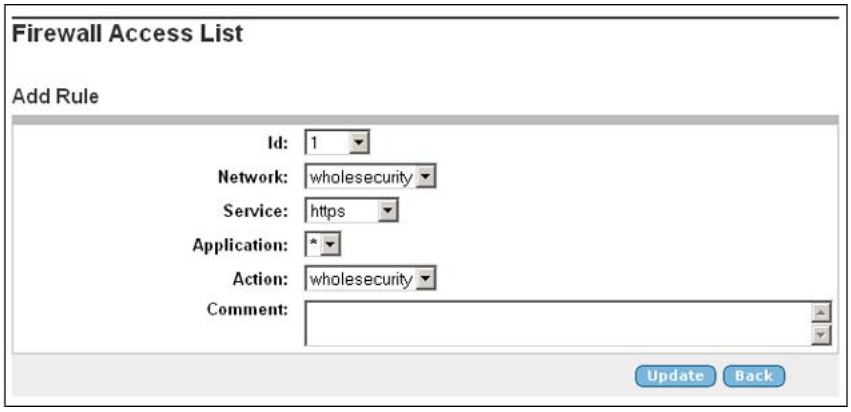
14. In the **Service** list box, select **https** .

    This means that access will be limited to the HTTPS protocol. Typically, the **https** service definition is available by default. If not, you can create this service definition (see Groups, Access Rules and Profiles on page 35.

15. In the **Application** list box, select the appspec definition called **WholeSecurity** .

    This is the appspec definition we created in the section Configure an Appspec Definition on page 246. By referencing this appspec definition in the access rule, access will be granted to the specified paths on the Confidence Online server and nothing else.

16. In the **Action** list box, select **Accept**.



17. Click **Update**.
18. Under settings, select **Groups**.

    The Groups form appears.
19. In the **Anonymous Group** list box, select **WholeSecurity** .

    The final step is to make the group we just created an anonymous group.
20. Click **Update** and apply the changes.

Result

As long as WholeSecurity is enabled and a Confidence Online server URL is specified, all requests for the VPN Portal will be redirected to the Confidence Online server. To limit access to just that server, all remote users are automatically placed in the anonymous group when pointing to the VPN Portal. The access rules of the anonymous group grants access to the Confidence Online server and nothing else.

Once the Confidence Online scan has been successfully performed, the remote user is allowed to log in to the VPN using the ordinary login screen. The user is then assigned his/her regular groups, granting access to additional sites and services.

Chapter 14: Branch Office Tunnels

In addition to IPsec-based user tunnels, where the remote user connects to the Avaya VPN Gateway (AVG) through an IPsec VPN client, the AVG also provides the ability to configure and establish IPsec-based branch office tunnels. Several peer-to-peer branch office tunnels can be configured for each virtual private network (VPN). Tunnels get automatically established whenever they are configured or when the system starts. Like user tunnels, branch office tunnels make use of a previously configured IKE profile. The IKE profile includes the preferred encryption settings for the tunnel.

Clustering Branch Office Tunnels

Branch office tunnels can co-exist with the clustering capabilities of the AVG. When there are more than one VPN Gateway in the cluster, and if several Portal IP addresses have been defined for a VPN, these IP addresses are evenly distributed among the AVGs on the public side of the cluster.

User clients, such as the Avaya IPsec VPN client (formerly Contivity), Net Direct and browsers, typically connect to the cluster by using a name registered in DNS. Round robin DNS is then used to spread out client requests evenly to the different cluster members. This is not applicable to branch office tunnels. Instead, one Portal IP address is configured (out of the list of IP addresses defined for the VPN) to be the endpoint for the tunnel. This IP address will always be brought up on one of the AVGs in the cluster. The branch office tunnel will be established from the AVG that currently owns the Portal IP address.

If a cluster member (AVG) fails, all Portal IP addresses will migrate to surviving cluster members. Because branch office tunnels are associated to a Portal IP address, any existing tunnels are likewise moved to the surviving AVG(s).

Scalability and Load Balancing

To achieve higher capacity, more AVGs can be added to the cluster. If there are two AVGs and both machines terminate a number of BO tunnels as well as regular IPsec/Net Direct/SSL, traffic capacity will increase by simply adding an AVG to the cluster.

Connection Example

Refer to Figure 5: Branch Office Tunnel on page 253.

1. A user working at the Headquarters (HQ) wishes to access a web server located at the Branch Office (BO). He browses to `http://accounting.denver.example.com` which corresponds to the IP address 10.1.2.10. The request is routed to the VPN Gateway.
2. The VPN Gateway finds a match between the user's source IP (10.0.1.19) and a local network specified in the BO tunnel profile configuration. The VPN Gateway also finds a match between the user's destination IP (10.1.2.10) and a remote network specified in the BO tunnel profile configuration.
3. The double match in step 2 means that the packets will be routed through the BO tunnel to the BO tunnel's endpoint. If Nailed Up tunnel mode is used, the packets will enter the tunnel instantly. If On Demand mode is used, there will be a slight delay before the tunnel gets established. The BO tunnel's endpoint is the branch office's public IP address (for example the Portal IP address of a VPN). This IP address should be specified as the remote IP address in the BO configuration on the HQ's VPN Gateway.
4. To authenticate to the BO endpoint, the HQ endpoint sends a shared secret (which has to be specified in the BO configuration at both endpoints). As an alternative, a string can be extracted from an X509 certificate and be matched against a string in the endpoints' BO configuration (see Connection Example).
5. The VPN Gateway (or corresponding device) at the BO endpoint routes the packets to their destination, that is 10.1.2.10.
6. For return traffic, the VPN Gateway at the BO endpoint recognizes 10.1.2.10 as belonging to a local network that is allowed to send traffic through the BO tunnel. The destination IP address (10.0.1.19) is recognized as belonging to a remote network in the BO configuration on the BO's VPN Gateway, so the packets are routed back through the BO tunnel.

   As we can see from the preceding example, the BO configuration on the HQ's VPN Gateway should be mirrored in the BO configuration on the BO's VPN Gateway (or corresponding device). Networks specified as remote networks on one endpoint should be defined as local networks on the other endpoint and vice versa.

   When a request is initiated from the branch office, the preceding steps are exactly the same, only reversed.

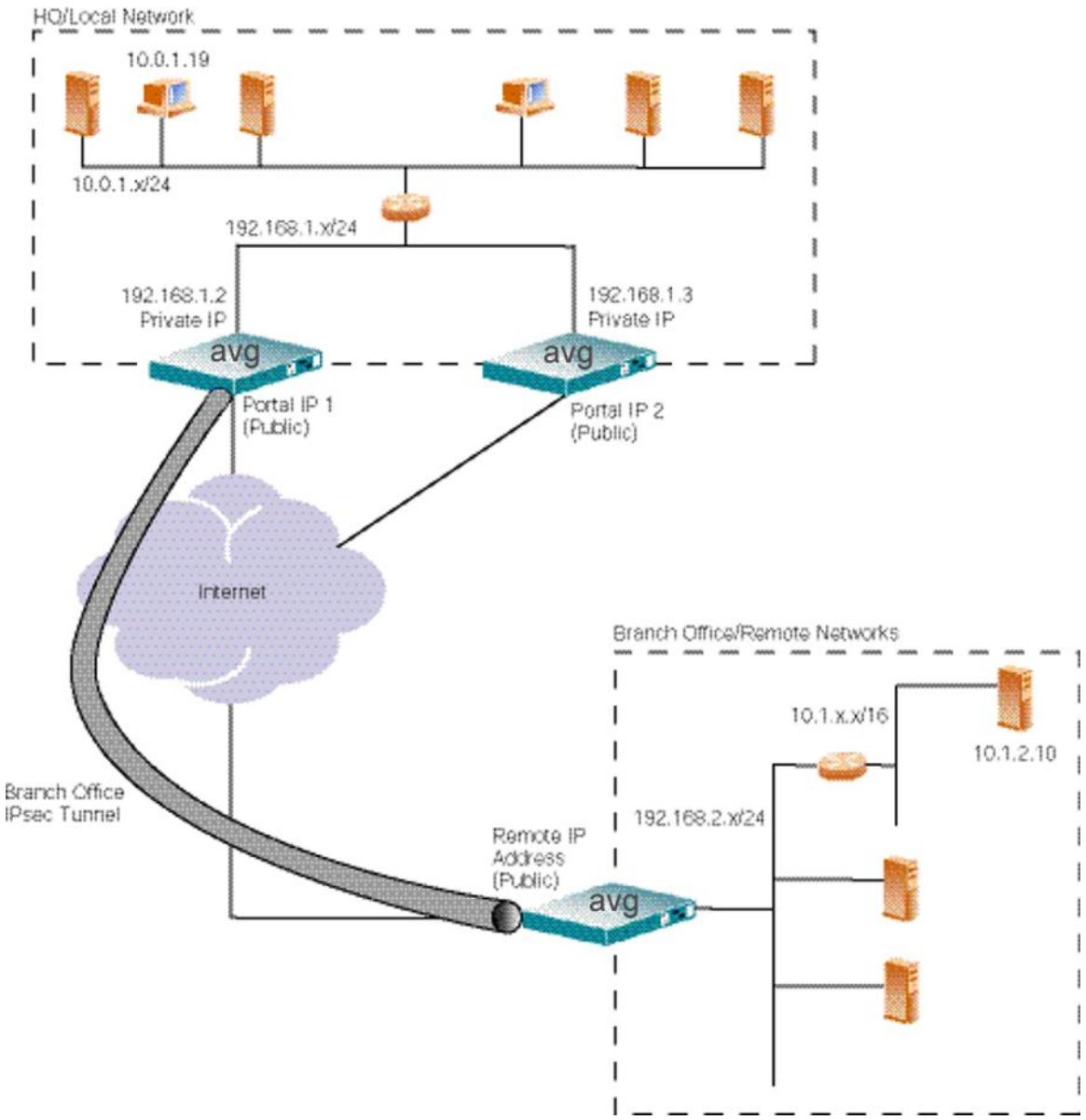


Figure 5: Branch Office Tunnel

The preceding configuration shows two VPN Gateways in a cluster. If the AVG that currently owns the BO tunnel fails, the tunnel migrates to the other AVG. For the networks on the private side to be aware of the tunnel shift and thus send the packets to the right AVG, the AVG will announce the branch office networks on the private side through RIPv2 messages.

Configuration Example

In this example we will create a branch office tunnel similar to that in the connection example in the previous section.

Configure Branch Office Tunnel

Branch office tunnels use IPsec for secure transfer of packets. To enable to the IKE daemon (IPsec server) on the VPN Gateway, proceed as follows:

Enable IPsec

Before you configure branch office tunnels, make sure IPsec has been enabled for your VPN by your Internet Service Provider (ISP).

Create Access Group

The purpose of creating an access group to be used by the branch office tunnel profile is to accomplish a more fine-grained access control to the remote networks at the branch office. The access rules of the group can for example grant or deny access to specific ports and protocols in the branch office networks. The group's access rules are applied when the response packets arrive at the local VPN Gateway.

For instructions on how to create access groups, see Groups, Access Rules and Profiles on page 35.

Create an IKE Profile

This step creates an IKE profile. If needed, several different IKE profiles can be created with different settings for encryption. The default settings for the IKE profile are usually fine for use with branch office tunnels. The NAT traversal options are however not applicable for branch office tunnels. For detailed information about available commands on the IKE profile menu, see the *Command Reference*.

If your ISP has already configured an IKE profile for use with your branch office tunnels you can skip these steps.

1. In the System tree view, select **VPN Gateways**.

The VPN Gateways form appears.

2. Select the configured VPN for which you to create an IKE profile.

   The VPN Summary form appears.

3. Under **Settings**, select **IP Sec**.

   The General form appears.

4. Select **IKE Profiles**.

   The IKE Profiles form appears.

5. Click **Add**.

   The Add New IKE Profile form appears.

6. In the **Name** field, enter a name for the IKE profile.

7. Click **Update**.

   The IKE Profiles form is redisplayed with the new IKE profile.

8. Use the General, Auth and Encryption, Diffie-Hellman Group, NAT and Dead Peer forms to modify the IKE profile according to your needs.

   As mentioned previously, the default settings for the IKE profile are usually fine for use with branch office tunnels so generally you do not have to edit the settings

9. Click **Update**.

Create a Branch Office Tunnel Profile

This step creates a branch office tunnel profile. The profile defines different criteria for the IPsec tunnel, for example local and remote endpoint IP addresses, authentication method, local and remote networks and so on . For detailed information about available commands on the User tunnel profile menu, see the *Command Reference*.

1. In the System tree view, select **VPN Gateways**.

   The VPN Gateways form appears.

2. Select the configured VPN for which you to create an IKE profile.

   The VPN Summary form appears.

3. Under Settings, select **IP Sec**.

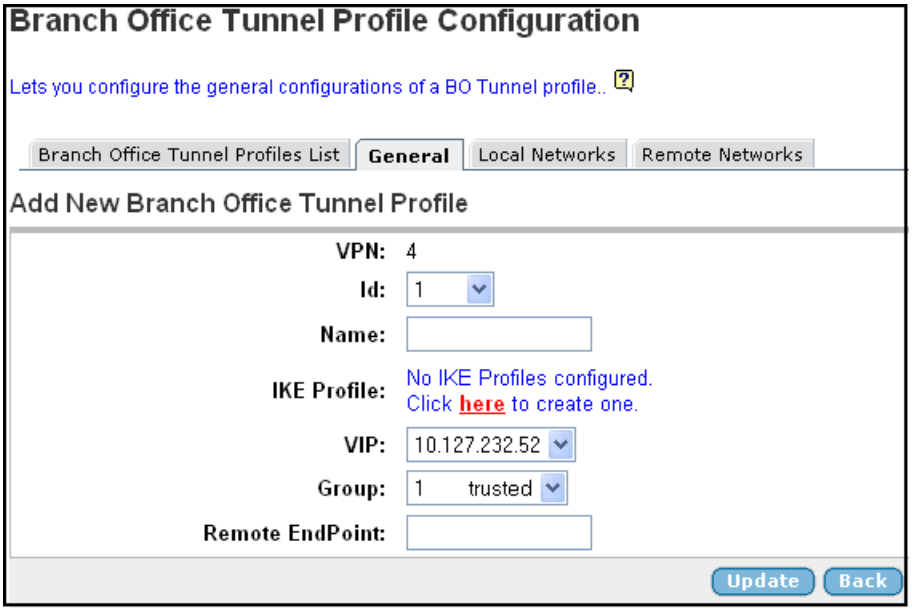
   The General form appears.

4. Select **BO Tunnel Profiles**.

   The Branch Office Tunnel Profiles form appears.

5. Click **Add**.

The Add New Branch Office Tunnel Profile form appears.



6. In the **Name** field, enter a name for the branch office tunnel profile.
7. In the **IKE Profile** list box, select the IKE profile we created in the previous section.
8. In the **VIP** list box, select the desired Portal IP address.

   This is the local endpoint's public IP address, that is the Portal IP address of your VPN.
9. In the **Group** list box, select the user access group whose access rules should apply.

   The group's access rules determine which ports and protocols will be available on the remote network. The rules are applied to packets coming out of the tunnel on their way back to the AVG.
10. In the **Remote Endpoint** field, enter the remote endpoint's public IP address.

    The BO tunnel's remote endpoint is the branch office's public IP address, for example the Portal IP address (or VIP) of a VPN.
11. Click **Update**.

    The branch office tunnel profile is added to the list.

Shared Secret Authentication

The authentication type is set to sharedsecret by default. As an alternative, the authentication type can be set to cert (see section).

1. In the System tree view, select **VPN Gateways**.

   The VPN Gateways form appears.
2. Select the configured VPN for which you to create an IKE profile.

   The VPN Summary form appears.
3. Under **Settings**, select **IP Sec**.

   The General form appears.
4. Select **BO Tunnel Profiles**.

   The Branch Office Tunnel Profiles form appears.
5. In the **Authentication Type** list box, verify that **sharedsecret** is selected.
6. In the **Shared Secret** field, enter the shared secret.

   This step sets the shared secret at the local endpoint. The same shared secret should be specified at the remote endpoint (for example a VPN Gateway or similar at the branch office).
7. Click **Update**.

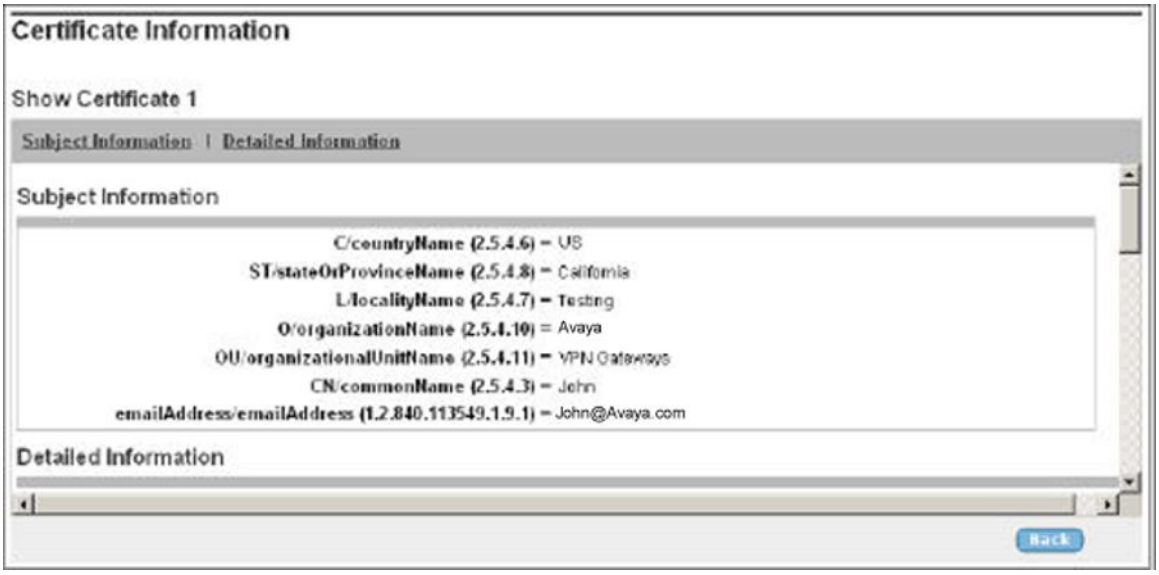
Certificate Authentication

When certificate authentication is used, the local endpoint sends a server certificate to authenticate to the remote endpoint and vice versa. Upon authentication, a value string is extracted from the certificate. This string is matched against a string specified in the endpoint's BO configuration. If a VPN Gateway is used to terminate the tunnel, the string that is used to match the remote certificate's string should be specified with the **`remoteid`** command.

1. In the System tree view, expand BO Tunnel Profiles and select **Branch Office Tunnel Profiles**.

   The Branch Office Tunnel Profile Configuration form appears.
2. In the **Authentication Type** list box, set the authentication type to cert. `cert`.
3. In the **Remote Certificate OID** field, specify the OID (or symbolic name) whose value should be extracted from the remote endpoint's certificate.

   Theoretically, if you imported the remote endpoint's certificate to the VPN Gateway you could find out the OIDs and their values for the certificate under **Certificates>Show**.



Example: L/localityName (2.5.4.7)=Testing 2.5.4.7 is the OID and **Testing** is the value.

In the preceding example, the value specified for **L/localityName** in the certificate is **Testing**. If **2.5.4.7** is specified as Remote Certificate OID, the value **Testing** will be extracted from the certificate and matched against the string specified in the **Remote ID** field.

4. In the **Remote ID** field, enter the string to match the value extracted from the remote endpoint's certificate.

   Using the preceding example, the string to enter can be **Testing**.

5. Click **Update**.
6. In the System tree view, under **IPsec**, select **General**.
7. Under **IPsec Certificate Settings**, in the **Certificate Number** field, select the desired server certificate.

   This is the server certificate that should be used to authenticate the VPN Gateway to the remote endpoint.

   To be able to select the certificate, it must exist on the VPN Gateway. See the "Certificates and Client Authentication" chapter in the *User's Guide* for detailed instructions on certificate management.

8. In the **CA Certificates List**, under **Available**, select the CA certificates(s) that should be used to authenticate the remote endpoint's certificate. Move it/them to the Selected list.

   To be able to select the CA certificate, it must exist on the VPN Gateway. See the "Certificates and Client Authentication" chapter in the *User's Guide* for detailed instructions on certificate management.

9. Click **Update**.

Configure Remote Networks

This step lets you configure the remote (branch office) networks that should be accessible through the branch office tunnel.

1. In the system tree view, under Branch Office Tunnel Profile, select the BO tunnel for which you wish to configure remote networks.

   The Branch Office Tunnel Profile Configuration is displayed.

2. Select **Remote Networks**.

   The Remote Networks form appears.

3. Click **Add**.

   The Add Remote Network form appears.

4. In the **Network IP** field, enter a remote network that should be accessible with the branch office tunnel.
5. Click **Save Network**.
6. The network is added to the Remote Networks list.
7. Add additional networks in the same way if needed.

Configure Local Networks

This step lets you configure the local networks that are allowed to send traffic through the branch office tunnel.

1. In the System tree view, under BO Tunnel Profile, select **Local Networks**.

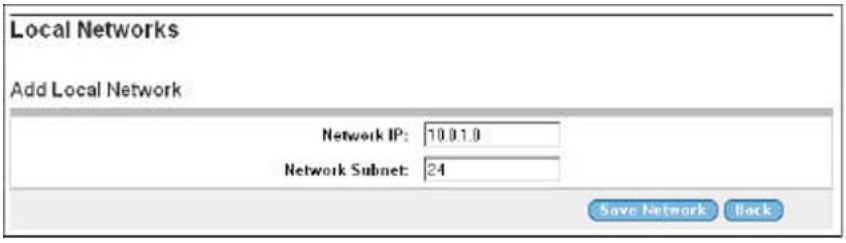
   The Local Networks form appears.

2. Select **Local Networks**.

   The Local Networks form appears.

3. Click **Add**.

   The Add Local Network form appears.



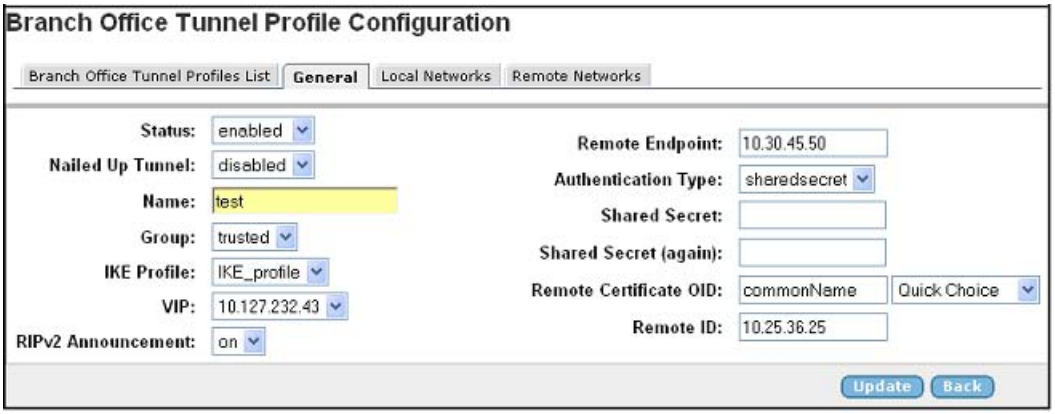
4. In the **Network IP** field, enter a local network that should be accessible with the branch office tunnel.
5. In the **Network Subnet** field, enter the desired network mask.
6. Click **Save Network**.

   The network is added to the Local Networks list.
7. Add additional networks in the same way if needed.
8. Apply the changes.

   For an explanation of BO Tunnel Profile menu options that have not been covered here, see the *Command Reference*.

RIP Announcement

1. In the system tree view, under **Branch Office Tunnel Profile**, select the BO tunnel for which you wish to configure RIP Announcement.
2. Select **General**.



3. In the **RIPv2 Announcement** list box, verify that the current RIP announcement setting is the desired one.

   - **on:** Branch office networks are announced on the private side through the RIPv2 protocol. The announcement is made on all interfaces for the relevant VPN except the traffic interface. This setting is required when the cluster consists of several AVGs.

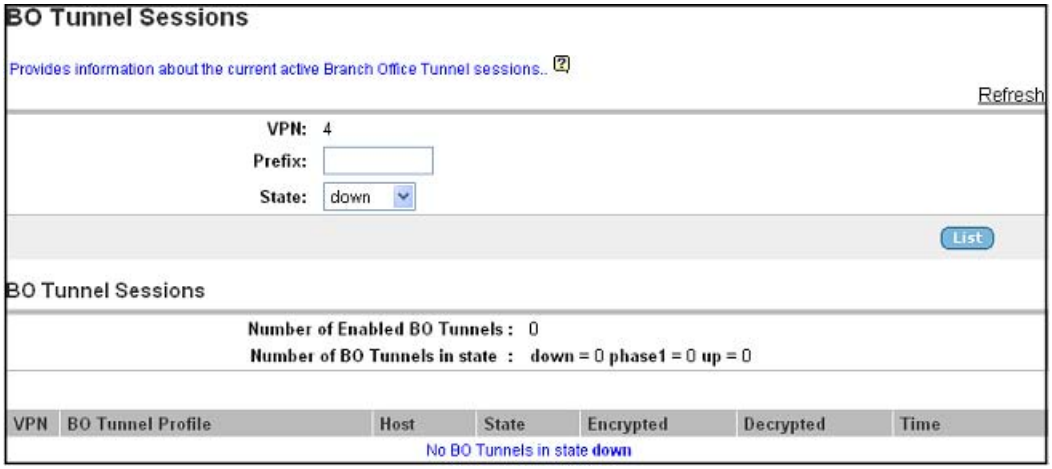
- **off:** Branch office networks are not announced on the private side. This setting may cause routing problems when the cluster consists of several AVGs.
- **all:** Same as on but the announcement is made on all interfaces.

4. Click **Update** and apply the changes.

Monitoring Enabled Branch Office Tunnels

To view the properties of enabled branch office tunnels, proceed as follows:

1. In the System tree view, expand **Monitor**.
2. Under **Monitor**, select **BO Tunnel Sessions**.



The output shows the name of the branch office tunnel profile, the AVG host from which the tunnel is set up, the tunnel state (**up**, **phase1** or **down**), encrypted data in kBytes and decrypted data in kBytes. The **up** tunnel state means that both ISAKMP and IPsec SAs are established, whereas the **phase1** state indicates that only the ISAKMP SA is established).

The output also shows the time the tunnel has been active (hours:minutes:seconds).

To limit the view to a specific VPN's BO tunnels, select the desired VPN in the VPN list box.

To limit the view to a specific BO tunnel, enter the name of the BO tunnel profile in the Prefix field. To limit the view to BO tunnel profiles beginning with a specific letter, enter for example d*.

To limit the view to BO tunnels in a specific state, select the desired state in the **State** list box.

Chapter 15: Transparent Mode

This chapter describes how to configure the system for use with the Avaya SSL VPN client and the Avaya VPN client (formerly the Contivity VPN client).

What is Transparent Mode?

The term "transparent" is mainly relevant from a user perspective. It means that the remote user will experience network access as if actually sitting within the corporate intranet. No Portal interaction is required.

As opposed to clientless mode, transparent mode requires the user to install one of the following VPN clients:

- Avaya SSL VPN client
- Avaya VPN Client (formerly the Contivity VPN client)

The Avaya VPN Gateway acts as the VPN server.

Transparent mode supports access to the intranet through legacy TCP- or UDP-based client applications. The following features and services can be used:

- Intranet Web browsing without logging in to the Portal.
- Intranet mail server access through the remote user's native e-mail client software.
- Telnet and SSH access to intranet terminal servers through the remote user's native Telnet or SSH client software.
- Access to a wide range of intranet services built on legacy client/server technology.

Avaya SSL VPN Client

As opposed to the Net Direct client (that can be downloaded for each user session and then removed), the SSL VPN client is permanently installed on the remote user's machine. Furthermore, it has a user interface and can be started without the user first having to log on to the Portal.

Note:

In later software versions, the Net Direct client is also available as a client to be installed permanently on the remote user's machine. See Net Direct on page 171.

The Avaya SSL VPN client comes in different versions:

- The LSP (Layered Service Provider) client. Compatible with Windows 98, ME, NT (with IE 5 or later) 2000 and XP. This client does not support UDP. The client is capable of sending version number and OS version to the AVG, which means that untrusted client versions and clients running on untrusted operating systems can be filtered out.
- The TDI (Transport Driver Interface) client. Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. The client is capable of sending version number and OS version to the AVG.
- Old clients, that is LSP and TDI clients that are not capable of sending version number and OS version to the AVG.

Server Configuration

The configuration on the VPN side is limited to enabling the different client versions and to paste the XML configuration file into the BBI once client configuration is completed (see step 10 on page 271).

Enable the Desired Client Versions

You can enable or disable client access based on client version. This example shows how to enable the TDI client. The procedure to enable access for LSP clients and old clients is the same.

1. In the System tree view, select **VPN Gateways**.

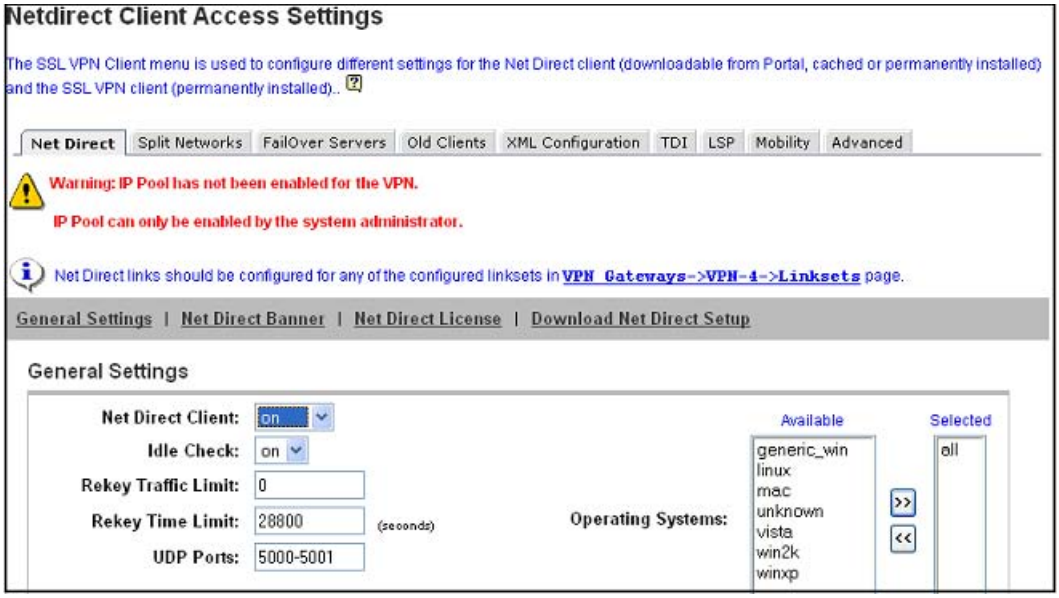
   VPN Gateways screen appears.

2. Select the VPN Gateway name.

   VPN Summary screen appears.

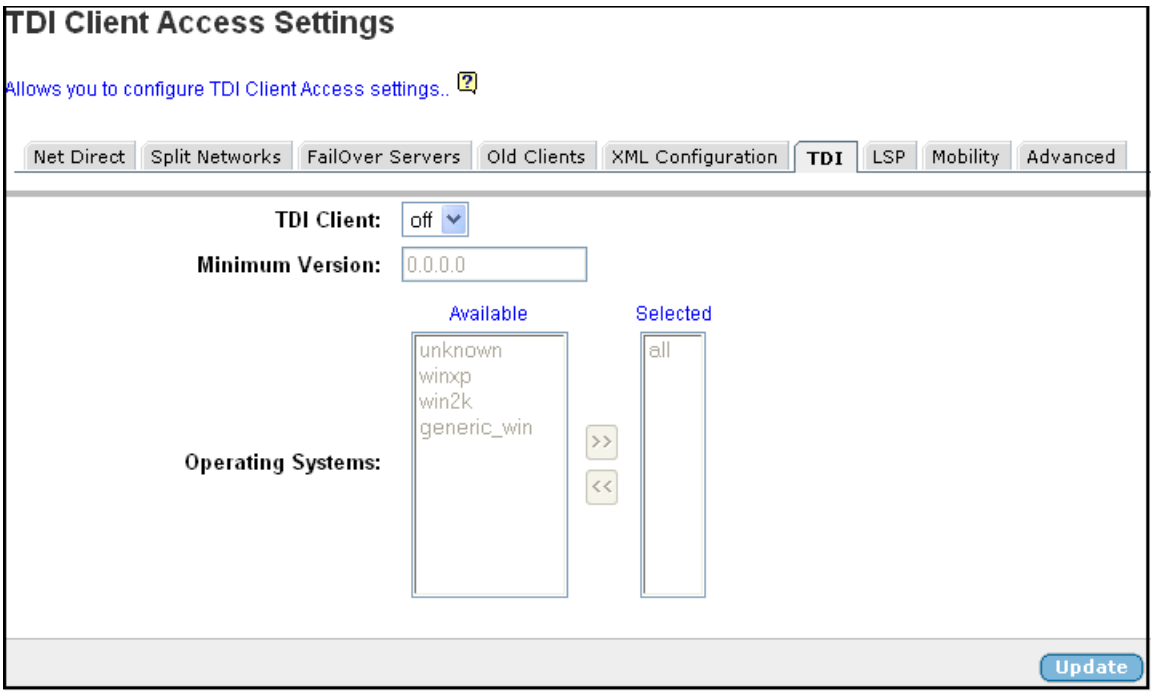
3. Under **Settings**, select **VPN Client**.

   Netdirect Client Access Settings screen appears.



4. Click on **TDI** tab.

   The TDI Client Access Settings form appears.



5. In the **TDI Client** list box, select **on**.

   By setting this parameter to on , users with TDI clients installed are allowed to access the VPN.

6. In the **Minimum Version** field, specify the minimum client version.

To restrict access to clients with a minimum version number, enter the desired version number. Example: If you enter **6.0.0.2**, only clients with this version number and higher are allowed to connect.

7. Move allowed operating systems to the Selected list.

   Only clients running on selected operating systems will be allowed to connect.

   - all: All client connections are allowed, irrespective of what OS the client runs on. Available for both TDI and LSP clients.
   - unknown: Clients running on an OS that cannot be identified (for example new OS versions) are allowed to connect. Available for both TDI and LSP clients.
   - winxp: Clients running on Windows XP are allowed to connect. Available for both TDI and LSP clients.
   - win2k: Clients running on Windows 2000 are allowed to connect. Available for both TDI and LSP clients.
   - win98: Clients running on Windows 98 are allowed to connect. Only available for LSP clients.
   - winnt: Clients running on Windows NT are allowed to connect. Only available for LSP clients.
   - winme: Clients running on Windows ME are allowed to connect. Only available for LSP clients.
   - generic_win: Clients running on any other Windows version are allowed to connect. Available for both TDI and LSP clients.

8. Click **Update** and apply the changes.

   To enable access for LSP clients or older versions of the TDI and LSP clients (released before the VPN Gateway 6.0 release), the procedure is the same. Only select **LSP Client** or **Old Clients** under **VPN Gateways>VPN Client** in the System tree view instead.

Enable Full Access

If not already active, the SSL VPN client can be started from the Portal's Full Access page (select **Full Access** on the **Access** tab). This however requires that the Full Access feature is enabled. When the SSL VPN client is started from the Full Access page, the remote user does not have to authenticate once again (in the SSL VPN client's login window) because he/she has already authenticated to the Portal.

For more information about starting the SSL VPN client from the Full Access page, see The Portal from an End-User Perspective on page 287.

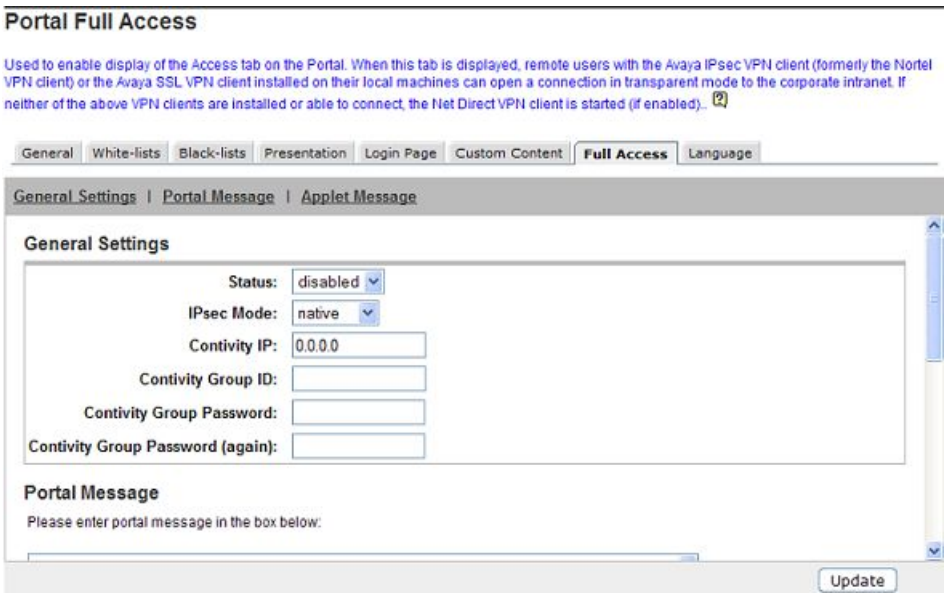
1. Follow the instructions for enabling SSL VPN client access previously in this chapter.
2. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
3. Select the VPN Gateway name.

   VPN Summary screen appears.
4. Under Settings, select **Portal**.

   Portal General Settings screen appears.
5. Click on **Full Access** tab.

   The Portal Full Access form appears.



6. In the Status list box, select **enabled**.
7. Click **Update** and apply the changes.

Note:

For the Full Access feature to work, the fully qualified domain name (FQDN) of the VPN Gateway must be specified as the server alias in the SSL VPN client (Servers tab>Add). See step 5 on page 268.

Client Configuration

To ensure that all users (for example in a specific user group) are provided with the same client settings is to install the SSL VPN client and make the desired settings. When done, a

configuration file in xml format can be exported and pasted into the CLI or the BBI. This makes the configuration available for download from the SSL VPN client, using the client's wizard.

This section describes how to configure the SSL VPN client. For options, buttons and so on that are not explained here, see the client's online help.

1. Install the SSL VPN client on your local machine. When installation is complete, the **SSL xtranet Configuration Wizard** screen appears:
2. Select **Manual configuration** and click **Finish**.
3. On the system tray, double-click the SSL VPN client icon.

   The Properties for SSL VPN client window appears:
4. Select the **Servers** tab and click **Add**. The **Add Server** screen appears.
5. In the **Alias** field, enter the VPN's fully qualified domain name (FQDN), for example vpn.example.com.

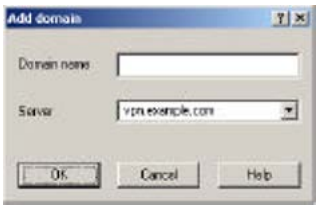
   Note:

   For the Full Access feature (see Enable Full Access on page 266) to work with the SSL VPN client, the fully qualified domain name (FQDN) of the VPN Gateway must be specified in the Alias field. Arbitrary aliases like "My intranet" will not work.
6. In the **Address** field, enter the VPN's Portal IP address.

   This IP address should be equivalent to the IP address specified under **VPN Gateways » VPN-1 » IPAddresses**.
7. In the **Port** field, enter 443 (HTTPS) as port number.
8. If required, make the desired settings for firewall traversal.

   For users working from a firewall-protected location, there are different options available for firewall traversal. By editing the server properties in the SSL VPN client, you will be able to configure the desired firewall traversal method. See the online help for detailed instructions.
9. Click **OK**, then **Apply**.
10. Select the **Name redirection** tab and click **Add**.

    This screen lets you add a domain for redirection of requests to the VPN server.



Example: Enter the domain name `example.com`. This will force all traffic using `example.com` in the address through the VPN server.

Fully qualified domain names (FQDN) can also be used, for example `www.example.com`.

11. Click **OK**.
12. Add another domain in the same way.

    The domain is added to the list on the **Name redirection** tab.

    The most qualified domain name in this list will be tried first, irrespective of order.

    Example: The domain name `support.example.com` is more qualified than `example. com.` When a domain name is given, the SSL VPN client will check if it matches the most qualified name first, because a less qualified name (like `example.com`) would match the given domain name in any case.

    If the remote user requests a domain name that is not listed on the **Name redirection** tab, the client will perform a DNS lookup to resolve the name to an IP address. This IP address will be checked against the routing rules defined on the **Routing** tab (if any).
13. Click **Apply**.
14. To configure IP address routing, proceed to the **Networks** tab and click **Add**.

    By configuring IP address routing you can specify whether requests to a specific network or address range should be redirected to the AVG server, blocked completely or passed through straight to its destination without the need to authenticate to the AVG server.
15. In the **Name** field, enter a suitable name for the network or address range.

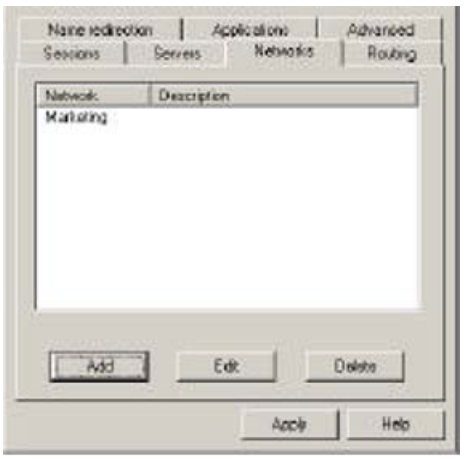
    This name will later be displayed on the Networks and Routing tabs.
16. In the **Comment** field, enter a description of the network (optional).
17. To register a specific network, select **Subnet**.

    Then enter the network's IP address and subnet mask.

    To register a range of networks, select Address range.

    Then enter the desired address range in the **From** and **To** fields. Example: To cover the entire Internet, enter 0.0.0.0 in the **From** field and 255.255.255.255 in the **To** field.
18. Click **OK** and **Apply**.

    The network is added to the **Networks** tab.



19. Proceed to the **Routing** tab and click **Add**.
20. In the **Network** list box, select the network for which you wish to add a routing rule.
21. To limit the routing rule to traffic to a specific TCP port, select the desired port in the Service list box (deselect the Use all ports check box first).

    If the desired TCP port does not exist in the list, enter the TCP port number directly in the list box. If the routing rule applies to all TCP ports, keep the tick in the Use all ports check box.
22. In the Redirect area, select the desired redirection rule for requests to this network.

    - Redirection through. Directs requests to the selected VPN server for authentication, provided the IP address corresponds to selected network or address range.

      Note:

      Requests using domain names listed on the Name direction tab will always be directed to the VPN server.
    - Direct connection. Directs the request straight to its destination, without going through the secure VPN Gateway connection.
    - Deny service. Any request with an IP address corresponding to a network or address range with this option selected will be denied.
23. Click **OK** and **Apply**.
24. Add another routing rule in the same way (start by defining the network or address range on the Networks tab).

    The routing rules are displayed on the **Routing** tab.

    The preceding routing rules say traffic destined for the intranet POP3 and SMTP mail servers as well as requests to the marketing network should be redirected through the VPN Gateway. Internet traffic is denied.

Export the Configuration File

When you have configured the SSL VPN client, you can export the configuration as an xml file and paste it into the CLI (or BBI).

1. Complete the configuration of the SSL VPN client and click **Apply**.
2. Select the **Advanced** tab and click the **Export config** button.
3. Save the file in xml format.

   If needed, several configuration files can be produced and exported if different user groups have different requirements.
4. Open the xml file in a text editor, for example Notepad and copy the contents.
5. Connect to the BBI.
6. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
7. Select the VPN Gateway name.

   VPN Summary screen appears
8. Under **Settings**, select **VPN Client**.
9. Click the **XML Configuration** tab.

   The XML Client Configuration form appears.
10. Under XML Client Configuration, paste the xml file into the field.
11. Click **Update**.
12. Apply the changes.

    The configuration is now available to remote users with the SSL VPN client installed. The configuration can be downloaded using the client's wizard (see next section). To install the client, the user must have administrator privileges.

Configure Client Using Wizard

If a configuration file has been produced and the contents have been pasted into the CLI (or BBI), remote users can download the configuration from the VPN Gateway through the SSL VPN client's wizard.

Note that this requires the VPN server to be configured as a portal server, which is normally the case.

The following instructions are directed to the remote user:

1. Install the SSL VPN client.

The wizard is displayed as the first screen.

If not, open the wizard by double-clicking the SSL VPN client icon on the system tray, go to the **Advanced tab** and click the **Wizard** button.

2. Click **Next**.
3. Specify the VPN's Portal IP address or domain name.
4. Click **Next**.

   The configuration is imported from the VPN Gateway.

SSL VPN Client from a User Perspective

1. Start the SSL VPN client.

   Double-click the **SSL VPN** client icon on your desktop or select the SSL VPN client program from the **Start** menu.

   The SSL VPN client icon appears on the system tray.

2. Connect to the desired server by entering a domain name or IP address in a TCP- or UDP-based application, for example a web browser.

   The SSL VPN client checks if the requested destination matches a domain name, network or IP address range configured in the SSL VPN client. If so, and if the client's routing rules say that requests for this network should be redirected to the VPN Gateway server for authentication, the **SSL VPN Client Authorization** dialog box appears.

3. Enter your user name and password and click **OK**.

Supplied credentials are checked against the configured authentication scheme, for example RADIUS or the VPN's local authentication database.

The Service list box may contain options for directing the user to a specific authentication database if several such databases exist in the configuration. In the BBI, this is configured in the **Display Name** field under **VPN Gateways >>VPN 1 >>Authentication>>(Method)>>General**.

When the remote user is successfully authenticated, a secure SSL tunnel is set up between the remote user's machine and the VPN Gateway. The requested resource is displayed (for example an intranet web page). If the user is not authorized to the resource, an error message will be displayed instead. If the requested address does not match a domain name, network or IP address range configured in the client, the user is directed straight to the destination without passing the VPN Gateway.

4. To logout from the VPN session, right-click the SSL VPN client icon on the system tray and select **Properties**.

   The Properties for SSL VPN Client window appears.

5. Select the **Sessions** tab.

   The name of the logged in user is displayed.

6. Click **Logout**.

Note:

The remote user is automatically logged out from the session if the idle timeout or maximum session length values are exceeded. These values can be specified on VPN level (under **VPN Gateways >>VPN 1 »General**), on group level (under **VPN Gateways » VPN-1 » Group-1 » Modify Group**) or on extended profile level (under **VPN Gateways>Group Settings>Groups>Extended Profile (Edit)**.

Avaya VPN Client

For users with the Avaya VPN client (formerly the Contivity VPN client) installed, access to intranet resources can be made available through the VPN Gateway through a secure IPsec connection.

Server Configuration

To enable the VPN Gateway to terminate IPSec VPN client connections, follow the following steps:

Note:

User name and password authentication is only supported if the user exists in the AVG's local database.

Create IP Pool

The IP pool comes into play when the remote user tries to access a host using the IPsec VPN client. A new IP address has to be assigned as source IP for the unencrypted connection between the VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

Several IP pools can be configured, each with a unique ID number and unique properties. By mapping the desired IP pool to a user group, you can create different methods for IP address and network attributes assignment for different user groups.

One of the configured IP pools should be selected as the default IP pool. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

The IP pools are used to assign IP addresses for Net Direct access as well (see Net Direct on page 171). If you have already configured an IP pool for use with the Net Direct client, this pool can also be used for the IPsec VPN client.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Select the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, select **IP Pool**.

   The IP Pool form appears.

4. Under **Default IP Pool** List, click **Add**.

   The IP Pool Configuration form appears.

The first available IP pool number is suggested in the IP Pool ID list box.

5. In the **Name** field, enter a name for the IP pool.

   By giving the IP pool a suitable name, it will be easier to recognize when selecting it in other forms.

6. In the **Status** list box, select **enabled** to enable the IP pool.

   If needed, you can later disable this particular IP pool without losing the other settings for the pool. When appropriate, you can then reenable the pool without having to configure all settings once again.

7. In the **Type** list box, specify how IP address and network attributes should be assigned to the client.

   Network attributes (including IP address) can be assigned either locally (using free IP addresses from your local subnet), from an external RADIUS server or from an external DHCP server.

   For IP pools of the local type, network attributes should be configured in the local system (see next section). For IP pools of the radius and dhcp types, network attributes can be configured on the local system as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute.

8. If needed, change the default proxy ARP setting.

   - on: Means that the VPN Gateway that handed out the IP address for a specific client connection will respond to ARP requests on behalf of the IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

   - off: Return traffic will reach its destination unless specific routes are configured.

   - all: Same as on but proxy ARP is used on all interfaces.

9. Click **Update**.

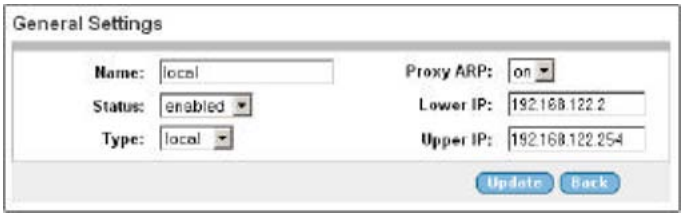
   Depending on which pool mechanism (local, radius or dhcp) you have selected, the IP Pool Configuration form now displays different input fields. Follow the relevant description depending on your choice.

Configure IP Address Range and Local Network Attributes

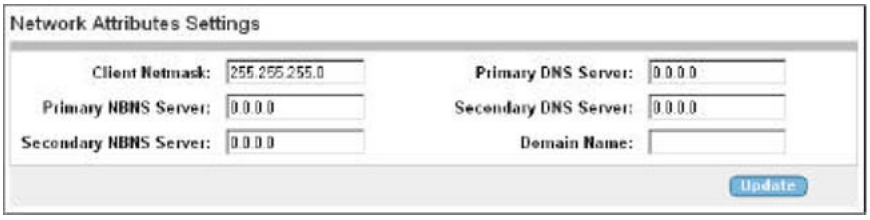
If you set the type of IP assignment to **local** (as described in step 7 on page 275 in the previous section), you should configure the desired IP address range. You can also configure network attributes to be retrieved from the system when the client connects.

If you set the source of IP assignment to **radius** or **dhcp**, continue with the relevant section (see the following pages) instead.

1. In the Lower IP and Upper IP fields, configure an IP address range.



2. Scroll down to Network Attributes Settings and configure the desired network attributes settings (optional).



The IPsec VPN client normally works fine without specific network attributes. You can however specify the desired network attributes in the form if needed.

- Client Netmask: Sets the network mask for the client. The network mask should cover the IP address range specified in 1 on page 276. The default network mask is `255.255.255.0`.
- Primary/Secondary NBNS server: Sets the IP address of a primary NBNS server (NetBIOS Name Server). Used if the IPsec VPN client should use a specific NBNS server to have computer names resolved into IP addresses. NBNS servers provide WINS (Windows Internet Naming Service) which is part of the Microsoft Windows NT server environment.
- Primary/Secondary DNS server: Sets the IP address of a primary DNS server. Use this command if the IPsec VPN client should use a specific DNS server to have domain names resolved into IP addresses. If no (primary or secondary) DNS server is specified here, the DNS server specified for the VPN to which the remote user belongs will be used. This is configured under **VPN Gateways>Gateway Setup>DNS**. (This option is only possible if a Secure Services Partitioning license is loaded). If only a default DNS server is specified (under **Network>DNS**), this will be used.
- Domain name: Lets you specify the name of the domain used while an IPsec user tunnel is connected. It ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

3. Apply the changes.

Configure RADIUS Network Attributes

If you set the IP pool's mechanism for network attributes assignment to radius, you should configure the VPN Gateway to retrieve network attributes from a RADIUS server.

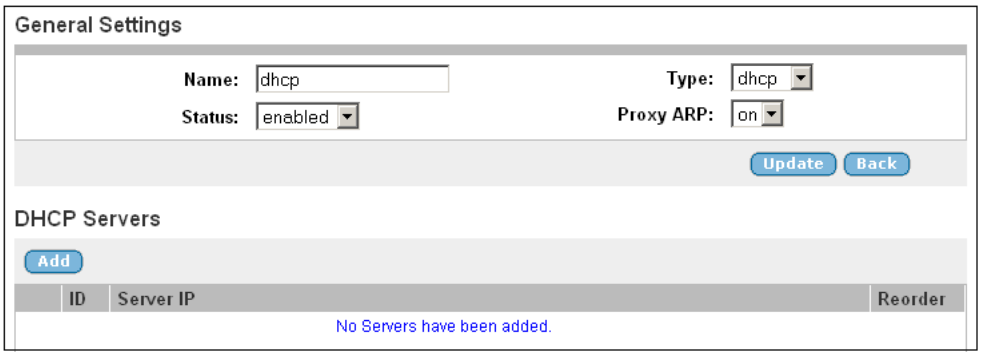
How to configure a RADIUS server (including network attributes) is described in Authentication Methods on page 75.

A minimum requirement is to configure retrieval of client IP address and primary DNS server. You can retrieve a number of network attributes, for example primary/secondary DNS server, primary/secondary NBNS server and so on .

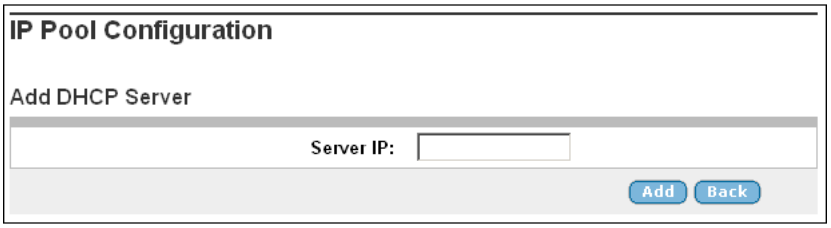
Network attributes can also be configured on the local system as fallback values if the RADIUS server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the local type (see step 2 on page 276 for instructions).

Configure DHCP Network Attributes

If you set the source of IP assignment to dhcp (as described in the section Create IP Pool on page 274), you should configure the VPN Gateway to retrieve network attributes from a DHCP server.



1. Under DHCP Servers, click **Add**.
2. Configure the external DHCP server IP address.



3. Click **Add**.
4. Apply the changes.

Network attributes can also be configured on the local system as fallback values if the DHCP server does not return a specific setting for a network attribute. This is

done in the same way as for IP pools of the local type (see step 2 on page 276 on step 2 on page 276 for instructions).

Create Default IP Pool

One of the configured IP pools should be selected as the default IP pool. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

2. Select the VPN Gateway name.

   VPN Summary screen appears.

3. Under **Settings**, select **IP Pool**.

   The IP Pool form appears.

4. In the **Default IP Pool** list box, select an existing IP pool as the default IP pool.
5. Click **Update**.
6. Apply the changes.

Map the IP Pool to User Group (Optional)

As mentioned on Create IP Pool on page 274, several IP pools with different mechanisms (that is local, radius or dhcp) can be configured. By mapping the IP pools to different user groups you can provide different ways of assigning IP address and network attributes depending on the user's group membership.

It is not mandatory to map an IP pool to a group. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool. How to create a default IP pool is described in the next section.

This is how to map an IP pool to a user group:

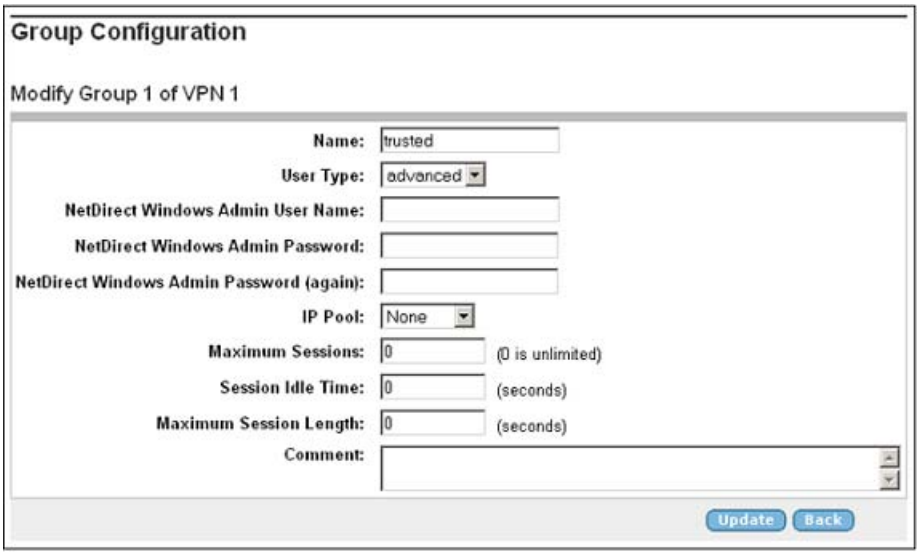
1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
2. Select the VPN Gateway name.

   VPN Summary screen appears.
3. Under **Settings**, select **Groups**.

   The Groups form appears.
4. Select the check box next to the group to which you want to map an IP pool.
5. Click **Edit**.

   The Modify Group form appears.
6. In the **IP Pool** list box, select the IP pool that you wish to map to the current group.



7. Click **Update**.
8. Apply the changes.

   Members of the current group will now receive IP address and network attributes from the selected IP pool when connecting to the VPN using their IPsec VPN clients.

Create an IKE Profile

Your ISP may already have configured an IKE profile and a user tunnel profile (see next section). If so, go directly to the section Configure Group to Use User Tunnel Profile on page 281 to map the user tunnel to the desired user group.

The default settings for the IKE profile are usually fine for use with the IPsec VPN client. If needed, several different IKE profiles can be created with different settings for encryption, NAT traversal and so on .

1. In the System tree view, select **VPN Gateways**.

   The VPN Gateways form appears.
2. Select the configured VPN for which you to create an IKE profile.

   The VPN Summary form appears.
3. Under **Settings**, select **IP Sec**.

   The General form appears.
4. Select **IKE Profiles**.

   The IKE Profiles form appears.
5. Click **Add**.

   The Add New IKE Profile form appears.
6. In the **Name** field, enter a name for the IKE profile.
7. Click **Update**.

   The IKE Profiles form is redisplayed with the new IKE profile.

Create a User Tunnel Profile

Your ISP may already have configured an IKE profile (see previous section) and a user tunnel profile. If so, go directly to the section Configure Group to Use User Tunnel Profile on page 281 to map the user tunnel to the desired user group.

The user tunnel defines different criteria for the IPsec tunnel, for example split tunneling, client PC control and so on . The default settings for the user tunnel profile are usually fine for use with the IPsec VPN client.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
2. Select the VPN Gateway name.

   VPN Summary screen appears.
3. Under **Settings**, select **IP Sec**.

   General screen appears.
4. Click on the **User Tunnel Profiles** tab.

   The User Tunnel Profiles screen appears.

5. Click **Add**.

   The Add New User Tunnel Profile form appears.

6. In the **Name** field, enter a name for the user tunnel profile.
7. Click **Update**.

   The User Tunnel Profiles form is redisplayed with the new profile.

8. Click the name of the user tunnel profile.

   The User Tunnel Profile Configuration form appears.

9. In the **IKE profile** list box, select the IKE profile name we created in the previous section.
10. In the Enable Banner list box, select whether or not a banner should be displayed in the IPsec VPN client when the connection is established.

    If set to enabled, enter a text string of your own choice in the **Banner Display** field. The banner appears at the top of the IPsec VPN client upon login.

11. Click **Update**.

Configure Group to Use User Tunnel Profile

The purpose of the following configuration is to map a previously configured user tunnel profile (with an IKE profile) to the selected user group. The user group has to be configured on the VPN Gateway.

If you have not yet configured user groups, you can follow these steps once the desired groups have been configured. Group configuration is described in Groups, Access Rules and Profiles on page 35.

1. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.
2. Select the VPN Gateway name.

   VPN Summary screen appears.
3. Under **Settings**, select **Groups**.

   Group screen appears.
4. Click **Add**.

   Add a Group screen appears.
5. In the **Name** field, enter a name for group.
6. Click **Update**.

   Modify a group screen appears.
7. Click on **IPsec** tab.

   The IPsec form appears.
8. In the **Shared secret** field, enter the group secret (used for group authentication).

   The group password entered by the remote user in the IPsec VPN client should match the group secret configured here.
9. Confirm the shared secret in the field.
10. In the **Tunnel Profile** list box, select the user tunnel profile to be used for the current user access group.

    Reference the user tunnel profile you have previously created.
11. Click **Update**.

Client Certificate Authentication

For remote users to be able to authenticate to the VPN Gateway through client certificate authentication, follow these steps:

1. Log on as VPN portal user.
2. Choose **Tools**, **VPN Administration**.
3. Select **Config** tab.
4. In the System tree view, select **VPN Gateways**.

VPN Gateway screen is displayed.

5. Click on the VPN Gateway name for which authentication needs to be done.

   VPN Summary screen appears.

6. Under settings, select **Authentication**.

   Authentication Server screen appears.

7. Click **Add**.

   Add New Authentication server appears.

8. Select the Auth ID.
9. In the **Name** field, enter a name for the authentication method.
10. In the **Domain Name** field (optional), enter a domain name to be used by the current authentication method.
11. Click **Update**.

Enable Full Access

If not already active, the IPsec VPN client can be started from the Portal's Full Access page (select **Full Access** on the Portal's **Access** tab). This however requires that the Full Access feature is enabled.

The client is started in the background and instructed to connect to a Avaya VPN Router (in contivity IPsec mode) or to the VPN Gateway (in native IPsec mode). The remote user does not have to authenticate once again because he has already authenticated to the Portal.

For more information about starting the IPsec VPN client from the Full Access page, see The Portal from an End-User Perspective on page 287.

1. Follow the instructions for enabling IPsec VPN client access previously in this chapter.

   Note that this is not required if users are to run the IPsec VPN client towards a Avaya VPN Router (formerly Contivity).

2. In the System tree view, select **VPN Gateways**.

   VPN Gateways screen appears.

3. Select the VPN Gateway name.

   VPN Summary screen appears.

4. Under Settings, select **Portal**.

   VPN Summary screen appears.

5. Select **Full Access**.

Portal General Settings screen appears.

6. Click on **Full Access** tab.
7. In the Status list box, select **enabled**.
8. In the IPsec mode list box, select the desired IPsec mode.

   This step lets you select the desired IPsec mode for the IPsec VPN client, that is whether the client should connect to an existing Avaya VPN Router (formerly Contivity) or the VPN Gateway.

   - contivity: Instructs the IPsec VPN client to connect to a VPN Router. Proceed to step 9 on page 284 to configure VPN Router access.
   - native: Instructs the client to connect to the VPN Gateway. Click **Update** and apply the changes. Configuration is complete.
9. To complete the configuration when **contivity** mode is selected, enter the desired VPN Router IP address in the Contivity IP field.
10. For group authentication to the VPN Router, enter the desired group ID in the **Contivity Group ID** field.
11. In the **Contivity Group Password** field, enter the shared secret used for group authentication.
12. Enter the shared secret again to confirm.
13. Click **Update**.
14. Apply the changes.

Client Configuration

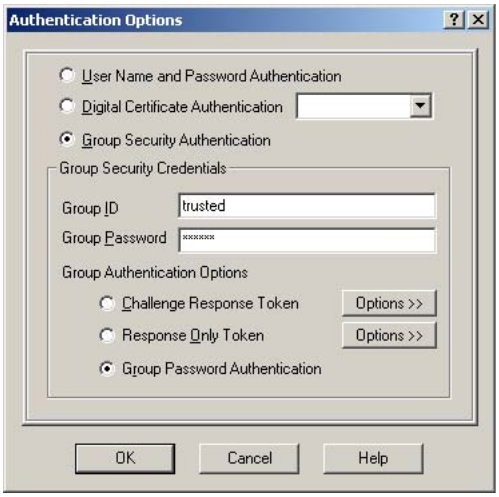
The IPsec VPN client can authenticate to the VPN Gateway in three ways:

- Group authentication
- User name and password authentication
- Client certificate authentication

Group Authentication

1. Create a new profile on the IPsec VPN client.

   On the **File** menu, select **New** and enter an appropriate connection name along with user name and password. In the **Destination** field, enter the VPN's IP address or DNS name.
2. On the **Options** menu, select **Authentication Options**.



3. Select the **Group Security Authentication** option.
4. In the **Group ID** field, enter the name of the user group.
5. In the **Group Password** field, enter the shared secret created in the section Server Configuration on page 273.
6. Under **Group Authentication Options**, verify that Group Password Authentication is selected.
7. Click **OK**.
8. Click **Save**.

User Name and Password Authentication

1. Create a new profile on the IPsec VPN client.

   On the File menu, select **New** and enter an appropriate connection name along with user name and password. In the **Destination** field, enter the VPN's IP address or DNS name.
2. Click **Save**.

Note:

User name and password authentication is only supported if the user exists in the AVG's local database.

Client Certificate Authentication

Make sure that both the client certificate and the CA certificate used to sign the client certificate are installed on the remote user's Windows machine.

1. Create a new profile on the IPsec VPN client.

   On the **File** menu, select **New** and enter an appropriate connection name along with user name and password. In the **Destination** field, enter the VPN's IP address or DNS name.
2. On the **Options** menu, select **Authentication Options**.
3. Select the **Digital Certificate Authentication** option.
4. In the list box to the right, select **MS CAPI** and click **OK**.

   The IPsec VPN client main window is redisplayed. The **User Name** field is now changed to Certificate.
5. Next to the Certificate field, click the icon depicted and select **Open**.

   Available client certificates are displayed.
6. Select the desired client certificate and click **OK**.
7. Click **Save**.

Chapter 16: The Portal from an End-User Perspective

This chapter describes the Portal from a user perspective. It includes step-by-step instructions on how access intranet resources in clientless mode, for example through the Portal. For instructions on how to change the Portal's look and feel, see Customize the Portal on page 197 Chapter 8, "Customize the Portal .

Accessing the Portal Web Page

In clientless mode, no VPN client need to be installed on the remote user's machine. Instead, the remote user accesses intranet resources through a secure SSL connection through the Portal.

In the available web browser, the remote user should enter the domain address (for example https://vpn.example.com) or IP address (for example https://192.168.128.100) to the AVG.

The Portal login page appears.

1. To log in, the remote user should enter his or her user name and password in the **Username** and **Password** fields, respectively.

   The user's credentials will be checked against a previously configured user record in the AVG 's local authentication database or in an external authentication database (for example RADIUS, LDAP, Netegrity SiteMinder, NTLM, RSA ClearTrust or RSA SecurID).

   Note:

   If a secondary authentication method is configured, an extra password field is displayed. The first field (Passcode) is used to authenticate to the primary authentication scheme and the second field (Password) is used to authenticate to the secondary authentication scheme. This feature is primarily designed to support single-sign on to backend servers in cases where the first authentication method is token-based or uses client certificate authentication. A secondary authentication server can only be specified for RSA SecurID, RADIUS and client certificate authentication mechanisms.

Configuring authentication methods is described in Authentication Methods on page 75.

2. To direct the remote user to a specific authentication database (if several different authentication methods are configured for the AVG), the corresponding option can be selected in the Login Service list box.

   To configure a suitable display name for the authentication method and to make it appear in the Login Service list box, go to the **VPN Gateways >>VPN 1 » Authentication(Method) »General** form and enter the desired name in the **Display Name** field (also see Authentication Methods on page 75.

   Note:

   If no display name has been configured for any of the authentication methods used, the Login Service list box will not be displayed.

3. Click **Login**.

   The Portal web page appears.

The Portal Web Page

Once the user is successfully authenticated, the Portal web page appears.

The Portal web page consists of different tabs from which the remote user can access intranet resources. What resources are available is determined by the access rules associated with the logged on user's group. See Groups, Access Rules and Profiles on page 35.

The Portal's look and feel can be customized with respect to language, logo, company name, colors and static text (see Customize the Portal on page 197.

Java Applet/ActiveX Control Icons

The icons to the right of the Portal tabs indicate whether or not certain Java applets and ActiveX controls are active:

Table 3: Java Applet/ActiveX Control Icons

	Avaya Endpoint Access Control Agent (EACA) running and checks have succeeded.
	EACA running and checks have failed.
	Citrix Metaframe support is enabled.
	The IE cache wiper is running.
	The Net Direct client is enabled on the VPN Gateway.

Avaya Endpoint Access Control Agent

Avaya Endpoint Access Control Agent (EACA) is a Java applet responsible for checking that the required components (executables, DLLs, configuration files, and so on .) are installed and active on the remote user's machine. For instructions on how to configure EACA, see Configure Avaya Endpoint Access Control Agent on page 217.

Citrix Metaframe Support

If Citrix Metaframe support is enabled, a Java applet will be started during login. This applet is not visible to the user and provides seamless support for securing Citrix client traffic through the VPN Gateway. The Citrix Metaframe support feature can be used with the Citrix Program Neighborhood as well as Citrix Nfuse, Citrix Web Interface and Citrix Presentation Server application portals through the internal or external Portal link types. See Group Links on page 127 Chapter 6, "Group Links " for instructions. Citrix Metaframe support is disabled by default (see **VPN Gateways >>VPN 1 »Portal »General**).

IE Cache Wiper

The IE cache wiper is an ActiveX control that clears the cache from HTML pages accessed during a Portal session (when running Internet Explorer). The Portal address is removed from the browser's visited URLs list when the user logs out or closes the browser window. The IE cache wiper is enabled by default (see **VPN Gateways >>VPN 1 »Portal »General**).

Net Direct Client

The Net Direct client is a VPN client similar to the Avaya SSL VPN client, only it does not require manual installation. The Net Direct client is temporarily downloaded to the remote user's machine and removed when the user exits the session. For instructions on how to configure the VPN Gateway for use with the Net Direct client, see Net Direct on page 171.

Capabilities

In clientless mode, the following services are enabled:

- Intranet web browsing.
- Access to SMB (Windows file shares) and FTP file servers.
- Intranet mail access through external web-based solutions, for example Outlook Web Access.
- Telnet and SSH access to intranet servers through terminal Java applet.

- Handling plugins, Flash and Java applets using HTTP proxy Java applet.
- Secure access to FTP file servers using native FTP client (FTP proxy).
- Port forwarding (application tunneling for third-party applications).
- Intranet access through native applications by downloading the Net Direct client

The Home Tab

The **Home** tab is the default tab on the Portal page.

The **Enter URL** field (configurable) lets the user access any web server through a secure SSL connection. The user should enter the address (with or without http://) and click **Go**. The client browser sends the request to the VPN Gateway as for example http://inside.example.com. A new browser window is opened, but now the request is rewritten with the AVG rewrite prefix (boldface) added, for example `https://vpn.example.com/http/inside.example.com`. This way, traffic is secured by the VPN Gateway.

Visited URLs can be saved as bookmarks by selecting the **Save as Bookmark** check box before clicking **Go** (see The Tools tab, Edit Bookmarks on page 293 for more information).

Links are defined within the context of a particular user access group, which means that all remote users who are members in that group will have access to the links you define.

Examples of l inks are:

- Secure link (through VPN Gateway) or direct link to web page
- Secure automatic logon link (through VPN Gateway) to password-protected web page
- Link to FTP or SMB file server
- Application tunnel link (port forwarder) through SOCKS encapsulated in SSL
- HTTP Proxy link (ensures display of web pages linked through plugins, e.g Flash)
- Link to Telnet or SSH terminal servers
- Net Direct link (downloads the Net Direct client)

See Group Links on page 127 for instructions on how to configure Portal links.

The Files Tab

The **Files** tab lets the user access a remote SMB (Windows file share) or FTP file server.

To access the file server, the user should do the following:

1. Enter the host name or IP address of the file server in the **Host** field. Also select the desired file server type, that is SMB (Windows file share) or FTP.
2. To display more options, select the **More options** check box.
3. To limit the view to a specific user's home share folder, enter the user's name in the **[Share]** field (optional). This field is ignored for FTP servers.

   To browse to a specific share folder, combine this field with the **[Path]** field.
4. To limit the view to specific workgroup, enter the workgroup's name in the **[Workgroup]** field (optional). This field is ignored for FTP servers.

   A window, containing the icons is displayed. These icons represents the hosts, which are the members of the icons.
5. Click on the **host** icon.

   User gets connected to the host.
6. Browse the shares on that host.
7. To specify a path to a specific folder, enter the desired path in the **[Path]** field. This field is dependent on what is entered in the **[Share]** field.

   For example, to browse to the folder `/temp/mystuff` under the share folder john, enter`john` in the **[Share]** field and **`/temp/mystuff`** in the **[Path]** field.
8. To make the file server accessible through a Bookmark (selectable from the Home tab), select **Save as Bookmark**.

   For a detailed explanation of the **Save as Bookmark** option, see The Tools tab, Edit Bookmarks on page 293.
9. Click **Open**.

   Files and folders in the specified folder are displayed by file type icon, file name, size, and date.

   If single sign-on is not allowed (for security reasons), an error message will be displayed. The user can still access the requested file server by entering the Portal password once again in the **Password** field and clicking **Open.**

   Domains for which single sign-on should be allowed can be added under **VPN Gateways >>VPN 1 »General »Single sign-on**.

   - To open a folder, click the folder name or icon.
   - To open/download a file from the file server to your computer, click the file name or icon.
   - To step up one level in the folder hierarchy, click **Up**.
   - To create a new folder on the file server, click **New Folder**. Then enter a folder name in the **Folder name** field. Finally click **Create**.

- To upload a file from your computer to the file server, click **Upload**. Locate the desired file in the window displayed. To upload the file to the current folder, click **Start Upload**.
- To delete a file or folder, select the corresponding check box and click **Delete**.
- To view files and folders as icons, select **icons** instead of **detail** in the list box to the right of the **Delete** option.
- To limit the view to files of a specific format, enter the desired file extension (for example .txt) after the * (asterisk) in the **Filter** field and press ENTER.
- To exit the file server session, select the session in the **File sessions** area and click **Close Session**.
- To add a new file server session, click **New Session**.

To simplify access, a link to the desired file server can be defined on the **Home** tab.

The Tools Tab, System Information

To view information about the current version of the AVG software, client information (for example login name and browser) and so on, select **System Info** on the **Tools** tab. The summarized information displayed on the System Information form provides an easy way for the user to obtain the relevant system data, for example when in contact with Support or Helpdesk personnel.

The System information tab also included an option to perform a bandwidth test. The result is displayed in Mb/s.

The Tools tab, Clear Login Cache

By selecting **Clear Login Cache** on the **Tools** submenu, the remote user has the option to clear the AVG system's cache from any kind of login information supplied during a Portal session.

The Tools tab, Change User Password

The **Change Password** option on the Tools submenu lets the remote user change his Portal password.

Note that this only applies if the user has logged in through the local database authentication method, that is his password stored in the VPN Gateway's local database.

The Tools tab, Edit Bookmarks

The **Tools** tab also includes an option to edit previously saved bookmarks. Both URLs entered on the **Home** tab and file server information entered on the **Files** tab can be saved as bookmarks.

Saving bookmarks from one session to another is only supported for users stored in an LDAP/Active Directory database. User preferences (such as bookmarks and login information supplied to other web servers during the Portal session) are saved to an attribute in Active Directory called isdUserPrefs.

To enable the User Preferences feature, you should set **User Preferences** to **enabled** under **VPN Gateways>Authentication>LDAP>General** in the BBI. You should also add the isdUserPrefs attribute to Active Directory (see Adding User Preferences Attribute to Active Directory on page 307 for instructions).

Saved bookmarks can later be selected in the **Go to** list box on the Portal's Home tab.

The Full Access Page

The **Full Access** page (select **Full Access** on the **Access** tab) provides a way for the user to launch his or her VPN client (if any) from within the Portal. Because the user has already logged in to the Portal, no further login to the VPN is required.

A VPN client connection enables the user to request resources as if working from within the intranet, that is no (further) Portal interaction is required. Supported VPN clients are the Avaya VPN client (formerly the Contivity VPN client), the Avaya SSL VPN client and the Net Direct client.

The **Access** tab is not displayed on the Portal by default, nor is VPN client access enabled by default. Follow the instructions in Transparent Mode on page 263 and Net Direct on page 171 respectively to enable access to the VPN from the **Access** tab, using the IPsec/SSL VPN clients and/or the Net Direct client.

To start a VPN client from the Access tab, the user should do the following:

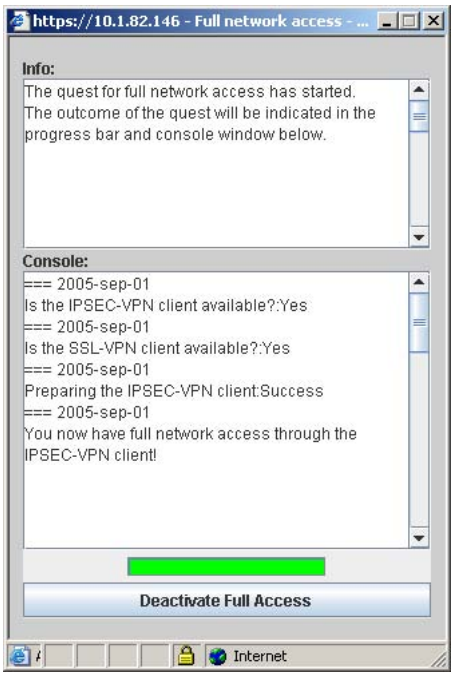
1. Click the **Yes** button.

   A Java applet is downloaded to the user's local machine. The Java applet checks if the IPsec VPN client is installed and able to connect to an Avaya VPN Router or to the VPN Gateway. If so, the IPsec VPN client is silently activated on the remote user's machine.

   If the IPsec VPN client is not installed on the remote user's machine or is unable to connect, the Java applet checks if the SSL VPN client is installed and able to connect to the VPN Gateway. If so, the SSL VPN client is silently activated on the remote user's machine.

If the SSL VPN client is not installed on the remote user's machine or is unable to connect, the Java applet goes on to check if the Net Direct client is enabled on the VPN Gateway and if it is able to connect. If so, the Net Direct client is silently activated on the remote user's machine.

When the user is successfully authenticated, a secure tunnel is set up between the user's local machine and the VPN Router/VPN Gateway.



2. Start a client application and request the desired intranet resource.

   The user's group membership determines his/her access rights.

3. When you are finished with the session, close the connection by clicking the **Deactivate Full Access** button in the Java applet window.

   The Java applet window is closed and the VPN client connection is terminated.

   If neither of the VPN clients are installed or able to connect, intranet resources can only be accessed in clientless mode, that is by requesting resources from the other Portal tabs.

The Advanced Tab, Telnet/SSH Access

The Telnet/SSH Access feature lets the user run a Telnet or SSH session to a specified server on the intranet. The session runs in a Java terminal emulation applet window. To simplify access, a link to the desired server can also be defined on the **Home** tab.

To enable display of applications with graphical user interfaces, SSH version 2 supports X11 forwarding.

To start a session, the user should do the following:

1. Enter the server's host name or IP address in the **Host** field.
2. Select the desired protocol (Telnet, SSHv1 or SSHv2).

   The typical Telnet/SSH port number is inserted in the **Port** field.
3. In the [**Log File Path**] field (optional), enter the path to the folder where the log file should be saved.
4. If the user has a non-standard keyboard, the [Keymap URL] field can be used to point to a keyboard mapping file located for example on an intranet file server.

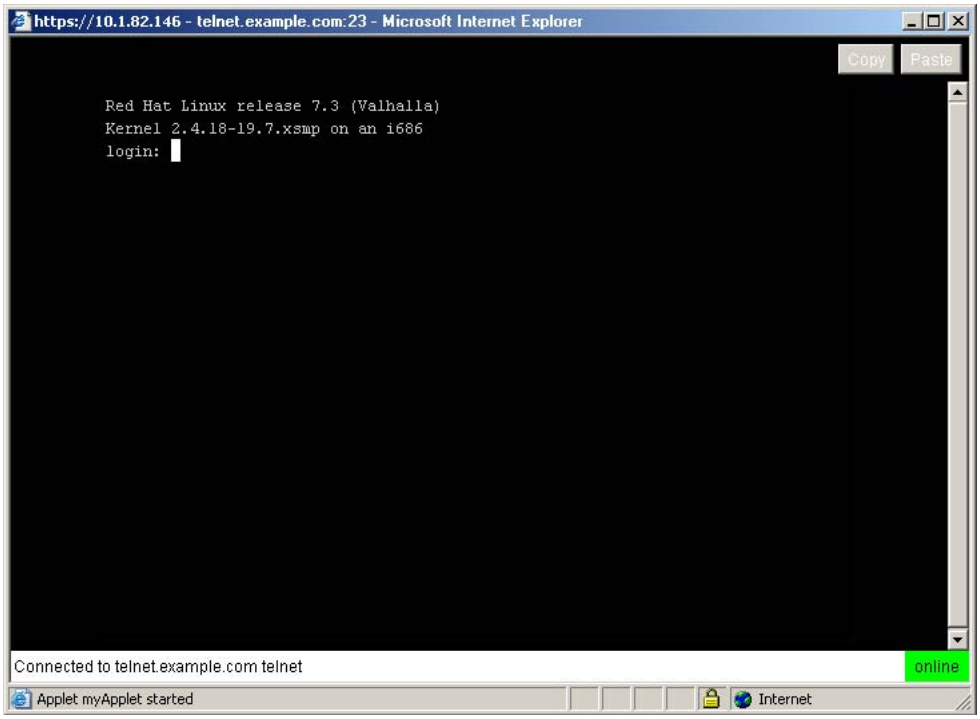
   Keystrokes to be sent to the remote server will automatically be translated to the proper keys. Syntax example: `http://inside.example.com/keyCodes.at386.`

   Documentation describing the configuration file properties in Syntax Description on page 315.
5. In the **[Proxy Host]** and **[Proxy Port]** fields, enter the IP address and port number of an intermediate Proxy server (if any) .

   Users who are working from a location requiring traffic to pass through an intermediate Proxy server on the intranet should enter the IP address (or domain name) and port of that Proxy server. All applet traffic will thus be tunneled to the AVG through the Proxy server. The Proxy server should have CONNECT support.

   Users should be informed if this step is required. If the Proxy Host and Proxy Port fields are left blank, all applet traffic will be tunneled directly to the AVG.
6. Click **Open**.

   This is what the Java applet window might look like when a Telnet session is started:



7. Click in the window to activate it before logging in to the terminal session.

   To quit the session, exit the terminal session and click the **Close** button top right.

The Advanced Tab, HTTP Proxy

We have previously described the **Home** tab, where the user can access intranet web pages in a secure mode. However, a web page may contain plugins (for example a Flash movie) which, in their turn, may include embedded links to other web pages. If a user executes such an embedded link, the HTTP request may not reach the VPN Gateway and the URL will not be displayed.

To ensure display of all URLs—also ones that are embedded in plugins—the HTTP Proxy feature lets the user download a Java applet to the client. The client browser's proxy settings should then be changed to direct all HTTP requests to this Java applet. The Java applet in its turn routes each request through a secure SSL tunnel to the AVG's proxy server, where it is unpacked and redirected to its proper destination.

To start a HTTP Proxy session, the user should proceed as follows:

1. In the **[Proxy Host]** and **[Proxy Port]** fields, enter the IP address and port number of an intermediate Proxy server (if any).

   Users who are working from a location requiring traffic to pass through an intermediate Proxy server should enter the IP address (or domain name) and port

of that Proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the Proxy server. The Proxy server should have CONNECT support.

Users should be informed if this step is required. If the Proxy Host and Proxy Port fields are left blank, all applet traffic will be tunneled directly to the VPN Gateway.

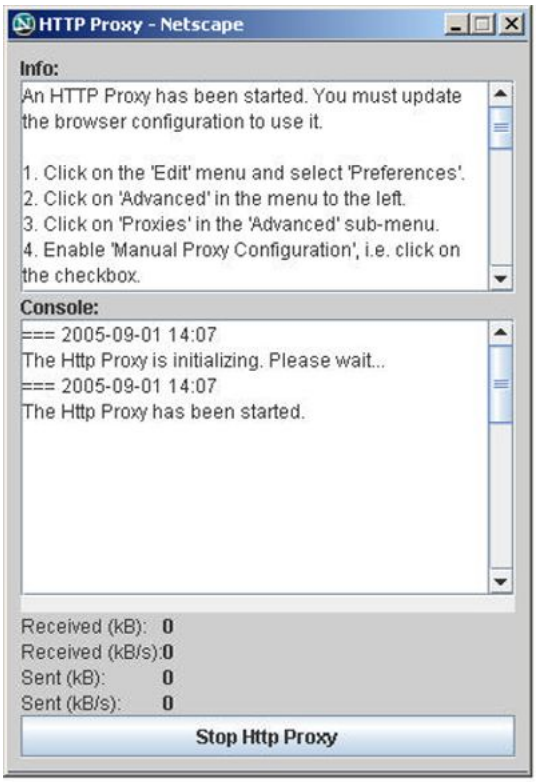
2. If Internet Explorer is used as the client browser, the user may select the check box Reconfigure Internet Explorer to use the HTTP Proxy.

   With this check box selected, the user does not have to change the browser's proxy settings manually, that is step 4 on page 297 following Step 4 can be ignored. Also, when the user exits the HTTP Proxy session, the browser's original proxy settings are automatically restored.

3. Click Open.

   The user will be asked to install a signed applet (certified by Avaya). When done, a Java applet window opens to confirm that an HTTP Proxy applet has been started.

4. Reconfigure the browser's proxy settings (not required for Internet Explorer).



Unless Internet Explorer is used as client browser (see Step 2), the browsers's proxy settings have to be reconfigured manually by the user.

Instructions (related to the type of browser used) are displayed in the Info part of the Java applet window. The example to the left shows how to change Netscape's proxy settings.

Having changed the proxy settings, the user can open a new browser window and surf the intranet in encrypted mode through the AVG's HTTP Proxy. The Java applet window and the Portal session must be active.

To quit the HTTP Proxy session, the user should click the Stop Http Proxy button in the Java applet window. If the browser was reconfigured manually, the user should also change the browser settings back to the original settings.

Note:

Outlook Port forwarder links (if configured) or Outlook Port forwarder Portal sessions (Advanced tab) will not work if a proxy server is configured in the client browser.

The Advanced Tab, FTP Proxy

The FTP Proxy feature lets the remote user access a remote FTP server through a native FTP client (installed on the remote user's machine).

When the FTP Proxy is started, a Java applet is downloaded to the client. The Java applet routes each request through a secure SSL tunnel to the AVG's proxy server, where it is relayed to the specified FTP server.

To start a FTP Proxy session, the user should proceed as follows:

1. In the **[Proxy Host]** and **[Proxy Port]** fields, enter the IP address and port number of an intermediate HTTP Proxy server (if any) .

   Users who are working from a location requiring traffic to pass through an intermediate HTTP Proxy server should enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

   Users should be informed if this step is required. If the Proxy host and port fields are left blank, all applet traffic will be tunneled directly to the VPN Gateway.

2. In the **Local Host** field, enter an IP address in the 127.x.y.z range (e.g `127.0.0.1`).

3. In the **Local Port** field, enter a free "local" port number.

   Port numbers just above 5000 are usually free to use. The application-specific port number for FTP is however recommended, so you can generally keep the suggested port number 21.

4. In the **Remote Host** field, enter the host name or IP address to the remote FTP server.

5. In the Remote Port field, enter the application-specific port number (that is 21 for an FTP session).

6. Click **Open**.

   The user will be asked to install a signed applet (certified by Avaya). When done, a Java applet window opens to confirm that an FTP Proxy applet has been started.

7. The user can now start his native FTP client.

   To access the remote FTP server the user should connect to the local host IP address specified in 2 on page 298.

8. To quit the FTP Proxy, the user should click the **Stop FTP Proxy** button in the Java applet window.

The Advanced Tab, Port Forwarders

Using the Port Forwarders tab, the user can set up a secure SSL connection to an intranet application server and run a TCP- or UDP-based client application. This is done by downloading a Java applet instructed to listen to a port number on the user's own computer. The applet then forwards all incoming traffic to the application server. The Port Forwarder tab includes the following options:

- Custom
- Outlook

Custom Port Forwarder

The Custom Port Forwarder lets the user start an optional TCP- or UDP-based application (for example native Telnet or Outlook Express). To start a custom port forwarder, the user should keep the **Custom** option in the **Port forwarder type** list box.

Example: Access to Outlook Express

In the following example, the user wishes to access the intranet's POP3 and SMTP mail servers using Outlook Express. The following information should be supplied:

1. In the [Proxy Host] and [Proxy Port] fields, enter the IP address and port number of an intermediate Proxy server (if any) .

   Users who are working from a location requiring traffic to pass through an intermediate Proxy server should enter the IP address (or domain name) and port of that Proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the Proxy server. The Proxy server should have CONNECT support.

Users should be informed if this step is required. If the Proxy Host and Proxy Port fields are left blank, all applet traffic will be tunneled directly to the VPN Gateway.

2. Under Mode, select the desired packet transfer protocol, that is **TCP** or **UDP**.
3. In the **Source IP** field, enter an IP address in the 127.x.y.z range (e.g `127.0.0.1`).
4. In the **Port** field, enter a free "local" port number, for example `5025`.

   Port numbers just above 5000 are usually free to use. The application-specific port number can also be used, e.g 25 for SMTP.
5. Usage of the [Host Alias] field (optional) is explained on the next page.
6. In the **Destination Host** field, enter the domain name (or IP address) of the intranet server you wish to connect to, for example **`pop3.example.com`**.
7. In the **Port** field, enter the application-specific port number (for example `110` for a POP3 session).
8. Click `Add` to display a second row of input fields for the next tunnel.

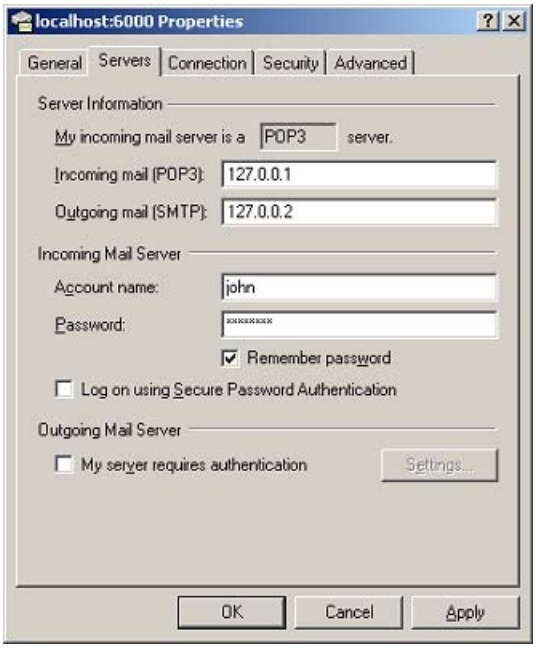
   To setup a connection to the SMTP server, enter a new IP address in the 127.x.y.z range in the Source IP field, for example `127.0.0.2.` Then enter a new port number in the **Port** field (for example `5026`). Finally enter the IP address or domain name to the SMTP server in the **Destination Host** field and the port to use in the Port field, in this case 25.

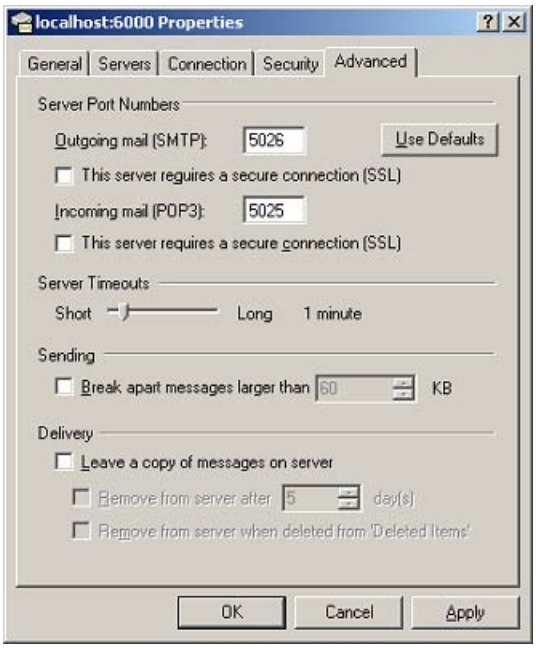
   Up to 16 tunnels can be created for one port forwarder.
9. Click **Start**.

   The user will be asked to install a signed applet for this session. By accepting, a Java applet window opens to confirm the information specified for the Port Forwarders.

Client Application Configuration (example)

Now the user has established two connections, one to the POP3 server and one to the SMTP server. In the client application, in this case Outlook Express, specify that incoming/outgoing mail is delivered/collected by hosts `127.0.0.1` and `127.0.0.2` respectively.





The port numbers to use are the ones entered in the "local" **Port** field for the POP3 and SMTP servers respectively, that is `5025` and `5026`. By entering the application-specific port numbers in the "local" **Port** field, that is `110` (for POP3) and `25` (for SMTP), existing port number settings in the mail client can be kept.

If the destination host is specified in the **Alias** field, and application-specific port numbers are used as "local" port numbers, no modifications to the client application are required. Note that use of host aliases is only possible if the user has administrator privileges on his client or has write access enabled for hosts and lmhosts files. Hosts and lmhosts files are located in

`%windir%\hosts` on Windows 98 and ME and in `%windir%\system32\drivers\etc\hosts` on NT, XP and Windows 2000.

To quit the Port Forwarder, the user should click the Stop Port Forwarder button in the Java applet window.

Telnet Port Forwarder

To establish a secure Telnet session using the Custom Port Forwarder, proceed as described, only enter the host address to the Telnet server in the **Destination Host** field (for example telnet.example.com) and port number 23 in the "remote" **Port** field instead. The user can then start the Telnet client and connect to for example `127.0.0.1 5025.` If the destination host is specified in the **Alias** field, the user can instead connect to the actual destination host and the local port number in the Telnet client, for example telnet.example.com 5025. If a short name is specified in the **Alias** field (for example `telnet`), the user can connect to telnet 5025 in the Telnet client.

HTTP Port Forwarder

To establish a secure HTTP session using the Custom Port Forwarder, proceed as described, only enter the host address to the Web server in the **Destination Host** field and port number 80 in the "remote" **Port** field instead. The user can then start his or her browser and type for example `127.0.0.1:5025` in the Address field. If the destination host is specified in the **Alias** field, the user can instead type the actual URL and the local port number in the browser's **Address** field, for example `www.example.com:5025`. If a short name is specified in the **Alias** field (for example web), the user can connect to `web:5025` instead.

Port Forwarder Links

To simplify access, Custom Port Forwarder links can be defined for display on the Portal's **Home** tab by the AVG operator. A Custom Port forwarder link can be defined to launch the application automatically (see Group Links on page 127 Chapter 6, "Group Links ").

Native Outlook Port Forwarder

The Outlook Port Forwarder lets the user start a native Outlook session to a specified Exchange server on the intranet. To start the Outlook Port Forwarder, the user should select the **Outlook** option in the **Port forwarder type** list box. This will display a different set of input fields.

Important:

For the Outlook Port Forwarder to work, the following prerequisites must be fulfilled:

- The Exchange server's domain name must be configured (**VPN Gateways »VPN 1>>Advanced>>DNS**). Using the preceding example, `example.com` should be entered in the **Search List** field. If several Exchange servers are used, all the Exchange servers' domain names must be configured in the DNS search list.
- The user must have administrator's rights on his/her computer or have write access enabled for hosts and lmhosts files. Hosts and lmhosts files are located in `%windir%\hosts` on Windows 98 and ME and in `%windir%\system32\drivers\etc\hosts` on NT, XP and Windows 2000.
- The Outlook Port forwarder is meant to be used by clients connecting to the AVG from outside the intranet. If the client has direct connectivity to the intranet, the port forwarder will fail. If the client has access to intranet DNS servers, communication will fail as well.
- The user's Outlook account must be hosted on the Exchange server(s) specified in the Port forwarder.
- The user's client machine must be of the Hybrid or Unknown node type. The node type can be checked by entering `ipconfig /all` at the DOS prompt.

  To change the node type to Hybrid (if needed), go to the registry editor folder `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`. If not already present, add a new DWORD Value called NodeType. Double-click NodeType and enter 8 in the Value Data field. Click OK and restart the computer.
- The Outlook Port forwarder will not work if a proxy server is configured in the client browser. This also means that a HTTP Proxy link or HTTP Proxy portal session (Advanced tab) cannot be active at the same time as the Outlook Port forwarder.
- If a firewall exists between the VPN Gateway and the Exchange server, the firewall settings must allow traffic to the required Exchange server ports. Note that these may vary with your environment. More information can be found at support.microsoft.com, for example Knowledge Base Articles 280132, 270836, 155831, 176466, 148732, 155831, 298369, 194952, 256976, 302914, 180795 and 176466.
- When a user clicks an embedded link in an e-mail message, the web site associated with the link must be displayed in a new instance of Internet Explorer. In Internet Explorer, go to the **Tools** menu and select **Internet Options**. Under the **Advanced** tab, go to **Browsing** and deselect the **Reuse windows for launching shortcuts** option.

The following information should be supplied by the user on the Port Forwarder tab:

1. Select the Start Outlook client check box if Microsoft Outlook should be started automatically when the Port Forwarder is started.
2. In the Source IP field, enter an IP address in the 127.x.y.z range (e.g `127.0.0.1`).
3. In the Exchange server (FQDN) field, enter the fully qualified domain name (FQDN) of the Microsoft Exchange Server, for example `exchange.example.com`.
4. Click **Add** to enter information for yet another Outlook Port forwarder (if required).

   Services provided (mail, calendar, address book and so on .) may be distributed between different Exchange servers. If this is the case, you have the option to create several Outlook port forwarders where the relevant Exchange servers can be specified.

   If several port forwarders are required, note that each port forwarder must have a unique source IP address. A new source IP address is automatically suggested by the system if you choose to add another port forwarder.
5. Click **Start**.

   The user will be asked to install a signed applet for this session.
6. Click **Yes**.

   A Java applet window opens to confirm the information specified for the Port forwarder(s). The user should carefully read the instructions, warnings and validation messages provided in the Java applet window. If the Port forwarder is not configured to start the Outlook client automatically, the user should wait until the applet is fully initialized before invoking the Outlook client manually.
7. Start the Outlook client (if not started automatically).
8. To quit the session, exit the Outlook client, then click the **Stop Port Forwarder** button in the Java applet window.

Note:

The user should not close the Java applet window as the last browser window, in which case the hosts files may not be cleaned up properly.

Logging out from the Portal

To logout from the Portal, the user should click the **Logout** prompt or the **exit** button top right.

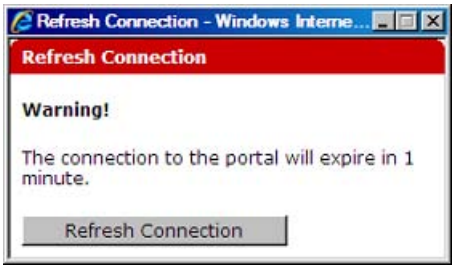
Idle Timeout

If the remote user has been idle longer than the time specified as default Session Idle Time for the VPN (under **VPN Gateways >>VPN 1 »General**), the user will be logged out

automatically. Note that session idle time can also be specified on group level (under **VPN Gateways >>VPN 1>>Group 1>>General**). Upon user login, the best idle time of the user's different groups and the default idle time for the VPN will be selected.

Maximum Session Length

The user is automatically logged out after the time specified as default Maximum Session Length for the VPN (under **VPN Gateways >>VPN 1 »General**), irrespective of the user being idle or not. Note that maximum session length can also be specified on group level (under **VPN Gateways >>VPN 1 »Group 1>>General**). Upon user login, the best maximum session length value for the user's different groups and the default maximum session length value for the VPN will be selected. 1 minute before the user is automatically logged out, a message is displayed. The message warns the user about the upcoming logout and offers to refresh the Portal connection.



IE Cache Wiper

Any HTML pages that have been accessed through the Portal will be cleared from the cache provided the Avaya cache wiper has been downloaded. The user – if running Internet Explorer – has the option to download the cache wiper when logging in to the Portal, if the **Use ActiveX Component For Clearing Cache** setting (under **VPN Gateways >>VPN 1 »Portal » General**) is enabled (enabled by default). The IE cache wiper also clears the browser history from entries accumulated during the Portal session. All previously recorded entries will remain.

If desired, the IE cache wiper can be enabled/disabled on group level instead of VPN level. Set **Use ActiveX Component For Clearing Cache** to group, then enable or disable the **Wiper** setting under **VPN Gateways >>VPN 1 »Group 1>>General**.

Appendix A: Adding User Preferences Attribute to Active Directory

For the remote user to be able to store user preferences on the Avaya VPN Gateway, you need to add the isdUserPrefs attribute to Active Directory. This attribute will contain an opaque data structure, containing various information that the user may have saved during a Portal session.

This description is based on Windows 2000 Server and Windows Server 2003. Make sure that your account is a member of the Schema Administrators group.

Install All Administrative Tools (Windows 2000 Server)

1. Open the Control Panel and double-click **Add/Remove Programs**.
2. Select **Windows 2000 Administrative Tools** and click **Change**.
3. Click **Next** and select **Install All Administrative Tools**.
4. Follow the instructions on how to proceed with the installation.

Register the Schema Management dll (Windows Server 2003)

1. Click **Start** and select **Run**.
2. In the **Open** field, enter `regsvr32 schmmgmt.dll`.

   Note that there is a space between regsvr32 and schmmgmt.dll.
3. Click **OK**.

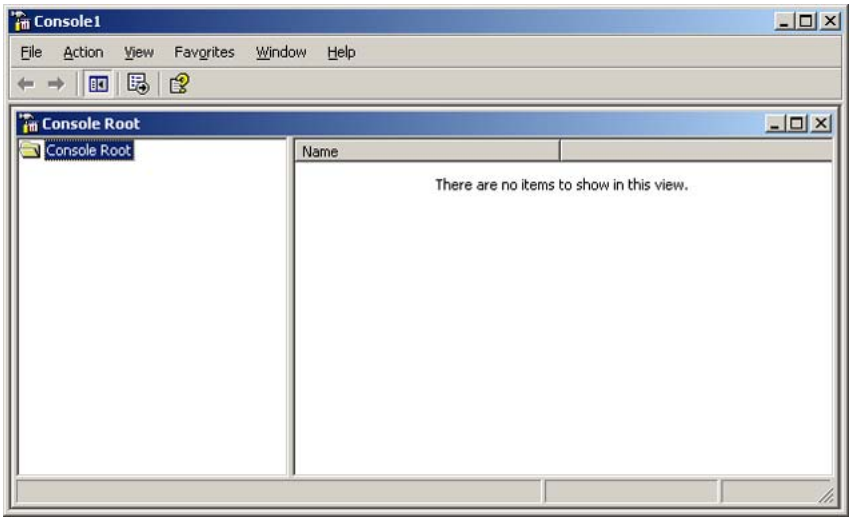
   This command will register schmmgmt.dll on your computer.

Add the Active Directory Schema Snap-in (Windows 2000 Server and Windows Server 2003)

1. Click **Start** and select **Run**.
2. On Windows 2000 Server, enter `mmc` in the **Open** field. On Windows Server 2003, enter `mmc /a` instead.

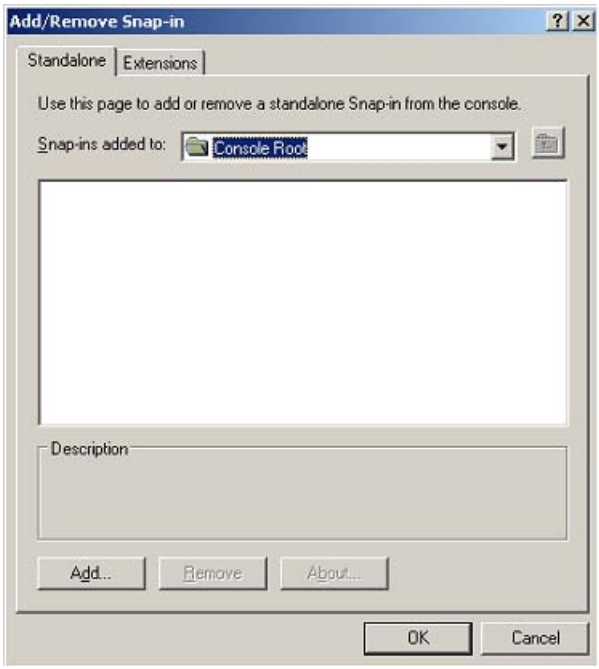
   Note that there is a space between `mmc` and `/a`.
3. Click **OK**.

   The Console window is displayed.



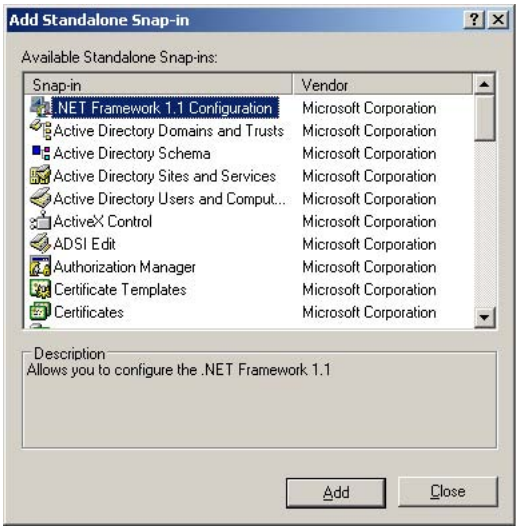
4. On the **File (Console)** menu, select **Add/Remove Snap-in**.

   The Add/Remove Snap-in window is displayed.



5. Click **Add**.

   The Add Standalone Snap-in window is displayed.



6. Under Snap-in, select **Active Directory Schema** and click **Add**.

   Active Directory Schema is added to the Add/Remove Snap-in window.

7. Click **Close** to close the Add Standalone Snap-in window.

   The Add/Remove Snap-in window is redisplayed.

8. Click **OK**.

   The Console window is redisplayed.

9. To save the console (including the Schema snap-in), go to the **File (Console)** menu and select **Save**.

   The Save As windows appears.
10. Save the console in the Windows\System 32 root folder.
11. As file name, enter `schmmgmt.msc`.
12. Click **Save**.

Create a Shortcut to the Console Window

1. Right-click **Start**, and select **Open all Users**.
2. Double-click the Programs and Administrative Tools folders.
3. On the **File** menu, point to New, and then select **Shortcut**.

   The Create Shortcut Wizard appears.
4. In the Type the location of the item field, type `schmmgmt.msc.`
5. Click **Next**.

   The Select a Title for the Program page is displayed.
6. In the Type a name for this shortcut field, type `Active Directory Schema.`
7. Click **Finish**.

Permit Write Operations to the Schema (Windows 2000 Server)

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

1. In the Console window, on the left pane, right-click **Active Directory Schema**.
2. Select **Operations Master**.
3. Select the check box The Schema may be modified on this Domain Controller.
4. Click **OK**.

Create a New Attribute (Windows 2000 Server and Windows Server 2003)

To create the isdUserPrefs attribute, proceed as follows:

1. In the Console window, on the left pane, expand Active Directory Schema by clicking the plus (+) sign.

   The Attributes and Classes folders are displayed.

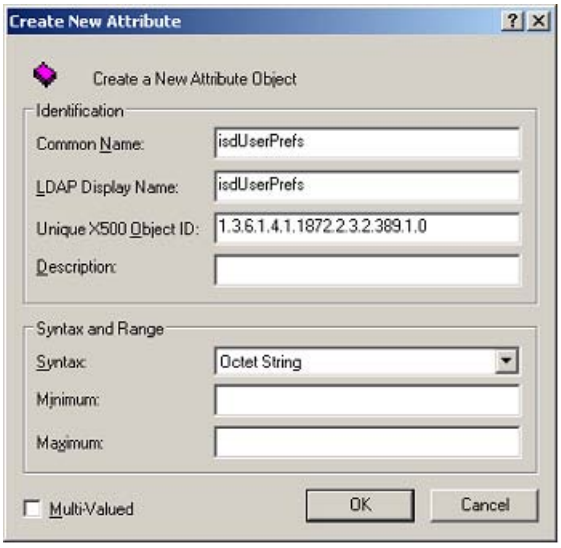
2. Right-click Attributes, point to New and select **Attribute**.

   You will now receive a warning that creating schema objects is a permanent operation and cannot be undone.

3. Click **Continue**.

   The Create New Attribute window appears.

4. Create the isdUserPrefs attribute as shown:



5. Click **OK**.

Create New Class

To create the avayaSSLOffload class, proceed as follows:

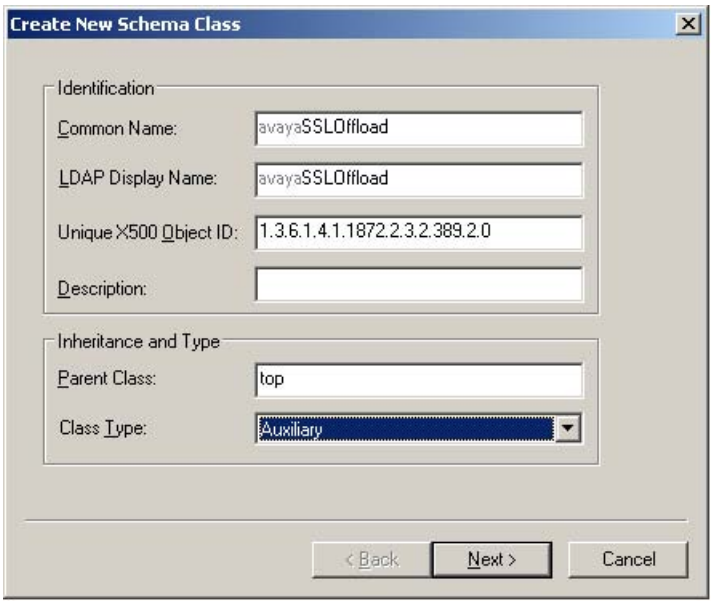
1. In the Console window, right-click **Classes**, point to **New** and select **Class**.

You will now receive a warning that creating schema classes is a permanent operation and cannot be undone.

2. Click **Continue**.

   The Create New Schema Class window appears.

3. Create the avayaSSLOffload class as shown:



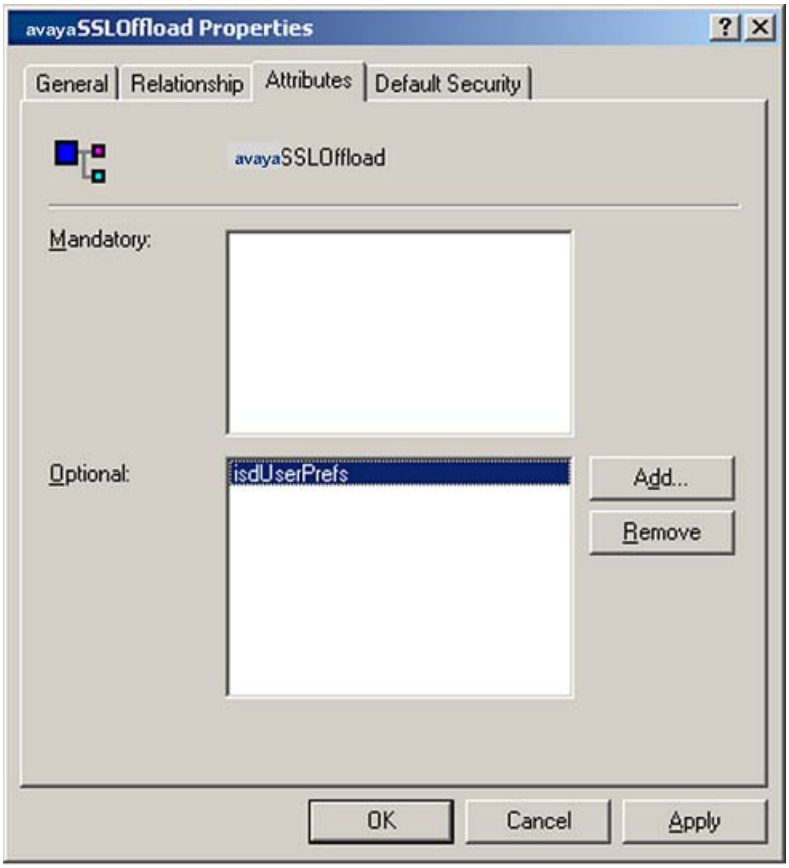
4. Click **OK**.

Add isdUserPrefs Attribute to avayaSSLOffload Class

1. In the Console window, on the left pane, expand **Classes**.
2. Select the **avayaSSLOffload** class.
3. Right-click and select **Properties**.

   The Properties window appears.

4. Select the **Attributes** tab and click **Add**.
5. Add the isdUserPrefs attribute as optional.



6. On the **Default Security** (Security) tab, set read/write permissions for the group that should have permission to write user preferences to the attribute.
7. Click **OK**.

Add the avayaSSLOffload Class to the User Class

1. In the Console window, on the left pane, expand **Classes** and select user.
2. Right-click and select **Properties**.

   The Properties window appears.
3. Select the **Relationship** tab.
4. Next to Auxiliary Classes, click **Add Class** (Add).
5. Add the avayaSSLOffload class as an auxiliary class. as shown:
6. Click **OK**.

   When you have enabled the User Preferences feature on the VPN Gateway (using the CLI command `/cfg/vpn #/aaa/auth #/ldap/enauserpre` or the BBI setting User Preferences under **VPN Gateways>Authentication>Auth Servers**

(LDAP)>Modify) the remote user should now be able to store user preferences in Active Directory.

Appendix B: Definition of Key Codes

Syntax Description

When using the Telnet applet available under the Portal's Advanced tab, there is an option to specify a keymap URL that points to a key code definition file. If your application uses a different keyboard layout than the standard VT320, a key code definition file can be created and uploaded to the keymap URL. This appendix shows how to create the key code definition file. Almost all special keys can be defined according to the following syntax rule:

[SCA] KEY=STRING

The characters enclosed in [and] are optional. Only one of the characters **'S'** (SHIFT), **'C'** (CTRL) or **'A'** (ALT) may appear before KEY, which is a textual representation of the key you wish to redefine (F1, PGUP and so on .).

The new STRING to be sent when pressing the key should come after the equals character (=). Hash marks (#) in the file declare the line as a comment and will be ignored. The following examples explain the syntax in more detail:

Send the string "test" when pressing the F1 key:

```
F1 = test
```

On pressing **Control + PGUP**, send the string "pgup pressed":

```
CPGUP = pgup pressed
```

Redefine the key **Alt + F12** to send an escape character:

```
AF12 = \\e
```

As can be seen, the string may contain special characters which may be escaped using the backslash (\).

Allowed Special Characters

The following table includes allowed special characters:

Note:

For some of the escape codes you need two backslashes, as these are specific javassh definitions not known by the Java Property mechanism.

Table 4: Allowed Special Characters

Special Character	Explanation
`\\b`	Backspace. This character is usually sent by the <- key (**Backspace** key).
`\\e`	Escape. This character is usually sent by the **Esc** key.
`\n`	Newline. This character will move the cursor to a new line. On UNIX systems, it is equivalent to carriage return + newline. Usually the **Enter** key send this character.
`\r`	Carriage Return. This key moves the cursor to the beginning of the line. In conjunction with Newline, it moves the cursor to the beginning of a new line.
`\t`	Tabulator. The tab character is sent by the **TAB** key and moves the cursor to the next tab stop defined by the terminal.
`\\v`	Vertical Tabulator. Sends a vertical tabulator character.
`\\a`	Bell. Sends a terminal bell character which should make the terminal sound its bell.
`\\number`	Inserts the character that is defined by this number in the ISO Latin1 character set. The number should be a decimal value.

Redefinable Keys

The following table explains which keys may be redefined. As explained earlier, each of the keys may be prefixed by a character defining the redefinition that occurs if it is pressed in conjunction with the SHIFT, CONTROL or ALT keys.

Table 5: Redefinable Keys

Key Representation	Remarks
`F1-F20`	The Function keys, that is F1, F2 and so on . up to F20.

Key Representation	Remarks
PGUP	The Page Up key.
PGDOWN	The Page Down key.
END	The End key.
HOME	The Home (Pos 1) key.
INSERT	The Insert key.
REMOVE	The Remove key.
UP	The Cursor Up key.
DOWN	The Cursor Down key.
LEFT	The Cursor Left key.
RIGHT	The Cursor Right key.
NUMPAD0-NUMPAD9	The numbered Numeric keypad keys.
ESCAPE	The Escape key.
BACKSPACE	The Backspace key.
TAB	The Tab key.

Example of a Key Code Definition File

Following is an example of the keyCodes.at386 key code definition file, created for an AT-386 Terminal.

```
#
F1=\\eOP
F2=\\eOQ
F3=\\eOR
F4=\\eOS
F5=\\eOT
F6=\\eOU
F7=\\eOV
F8=\\eOW
F9=\\eOX
F10=\\eOY
F11=\\eOZ
F12=\\eOA
#
# Shift F1 thru F10
#
SF1=\\eOp
SF2=\\eOq
SF3=\\eOr
SF4=\\eOs
SF5=\\eOt
SF6=\\eOu
SF7=\\eOv
SF8=\\eOw
SF9=\\eOx
SF10=\\eOy
SF11=\\eOz
SF12=\\eOa
#
# Other cursor movement keys
#
UP=\\e[A
DOWN=\\e[B
RIGHT=\\e[C
LEFT=\\e[D
#
INSERT=\\e[@
# REMOVE=\\177  #( hex 7F  /  Decimal 127  /  Octal  177  /
DEL Key)
#
HOME=\\e[H
PGDOWN=\\e[U
PGUP=\\e[V
END=\\e[Y
#
```

Appendix C: Using the Port Forwarder API

General

This appendix describes some of the tasks needed when using the Port Forwarder API. The JavaDoc will give you a more detailed view of the API.

The Port Forwarder API is used to provide tunnels through the Avaya VPN Gateway (AVG) without having to start any applets from the Portal. It can be used by any type of Java application or applet.

The tunnel specifications are set by defining a port forwarder in the CLI/BBI. It is then referred to when setting up the Port Forwarder API.

Note:

Defined applications are only started automatically if the port forwarder API is used by an applet.

The API and Demo application are available from the Portal. Example:

`https://vpn.example.com/avaya_cacheable/portforwarder.zip`

The zip file contains both a signed and an unsigned version of the API along with javadoc documentation and a demo application with source code.

Creating a Port Forwarder

The Port Forwarder API is a collection of functions used to provide applications with the ability to send traffic through a previously defined port forwarder link. For instructions on how to configure a port forwarder link on the AVG Portal, see the chapter "Group Links" in the *Application Guide for VPN*.

To be able to use the Port Forwarder API, two URLs are needed:

- URL for the Portal login (called loginUrl in the following examples)

  Example: `http://vpn.example.com/login_post.yaws?user=test&password=test&authmethod=default&url=`

  The parameters are the same as if accessing the Portal through a web browser.

- URL for the actual port forwarder (called portForwarderUrl in the following examples)

Example: `http://vpn.example.com/link.yaws?t=custom&a=1&b=1&c=1`

The parameters a, b and c in the second link point out the link according to:

a: VPN number b: Linkset number c: Link number

Demo Application

The Demo application is, in a simple way, showing how the Port Forwarder API is used. It can be run both as a regular application and by using the Java Web Start technology. It takes a couple of parameters needed to point out the Portal and link to use.

-vpnurl	The URL to the portal, for example `https://vpn.example.com`.
-linktype	The type of the link to use, for example "custom". The link type should be the same as defined in the CLI/BBI.
-vpn	The number of the VPN in the Portal, for example 1.
-linkset	The number of the linkset in the VPN, for example 1.
-link	The number of the link in the linkset, for example 1.

When run as a regular application, the arguments are simply passed on the command line:

```
java com.avaya.avg.demo.PortForwarderDemo -vpnurl
https://vpn.example.com -linktype custom -vpn 1 -linkset 1-link 1
```

For Java Web Start, parameters are passed through the jnlp file. A template jnlp file is provided along with a corresponding html file. For information aboutJava Web Start, refer to http://java.sun.com/products/javawebstart.

A correct jnlp file corresponding to the preceding example looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<jnlp spec="1.0+"
    codebase="https://vpn.example.com/"
    href="PortForwarderDemo.jnlp">
  <information>
    <title>PortForwarder Demo</title>
    <vendor>Nortel</vendor>
    <description>Demonstration of PortForwarder API</description>
  </information>
  <offline-allowed/>
  <security>
    <all-permissions/>
  </security>
  <resources>
    <j2se version="1.4+" />
    <jar href="signed_portforwarderdemo.jar"/>
    <jar href="signed_portforwarder.jar"/>
  </resources>
  <application-desc main-class="com.nortel.nvg.demo.PortForwarderDemo">
    <argument>-vpnurl</argument>
    <argument>https://vpn.example.com</argument>
    <argument>-linktype</argument>
    <argument>custom</argument>
    <argument>-vpn</argument>
    <argument>1</argument>
    <argument>-linkset</argument>
    <argument>1</argument>
    <argument>-link</argument>
    <argument>1</argument>
  </application-desc>
</jnlp>
```

The Custom Content concept (`/cfg/vpn #/portal/content`) can be used to host Java Web Start applications on the Portal. Building the demo project results in a content.zip file suitable for content area upload. A precompiled one is also provided. For the material in the content area to be cacheable by the client web browser, it has to be put in a top directory called "/avaya_cacheable".

The demo project zip file has such a directory at it's top level. When uploaded to the content area, the demo is accessible through:

`https://vpn.example.com/avaya_cacheable/PortForwarderDemo.html`

The provided build.xml file contains an example of how to create a content.zip file.

Creating a Port Forwarder Authenticator

A Port Forwarder authenticator must implement the PortForwarderAuthenticator interface:

```
public PortForwarderCredentials getCredentials();
public java.net.PasswordAuthentication getProxyCredentials();
```

Example

Following is an example of the code for creating a Port Forwarder authenticator.

```
private String getCookieFromURL(String spec) {
try {
URL url = new URL(spec);
URLConnection connection = null;
((HttpURLConnection) connection).setFollowRedirects(false);
connection = url.openConnection();
connection.getInputStream();
/* check if we are authorized */
if (connection != null) {
String headerField =
getHeaderField(connection, SET_COOKIE_HEADER);
return headerField.substring(headerField.indexOf('=') + 1,
headerField.indexOf(';'));
} else {
return null;
}
} catch (MalformedURLException e) {
e.printStackTrace();
} catch (IOException e) {
e.printStackTrace();
}
return null;
}
PortForwarderAuthenticator pfa =
new PortForwarderAuthenticator() {
public PortForwarderCredentials getCredentials() {
cookie = getCookieFromURL(loginUrl);
if (cookie == null) {
return null;
}
cred.setAvayaToken(cookie);
return cred;
}
public PasswordAuthentication getProxyCredentials() {
LoginDialog loginDialog = new LoginDialog();
return new PasswordAuthentication(loginDialog.getUserId(),
loginDialog.getPassword()
.toCharArray());
}
};
portForwarder.setAuthenticator(pfa);
```

Adding a Port Forwarder Logger

A Port Forwarder logger must implement the PortForwarderLogger interface:

```
public void log(int logLevel, int logCode, Object[] params, Throwable
throwable);
```

```
public void log(int logLevel, String msg, Throwable throwable);
```

The first function is used when the Port Forwarder logs a message in the Messages.properties file, that is messages of type PortForwarderConstants.LOG_LEVEL_INFO and PortForwarderConstants.LOG_LEVEL_ERROR and the second one is used for messages of type PortForwarderConstants.LOG_LEVEL_DEBUG and PortForwarderConstants.LOG_LEVEL_DEBUG_VERBOSE.

The PortForwarderLogger is added to the Port Forwarder by calling the setLogger function.

Example

Following is an example of the code for adding a Port Forwarder logger.

```
public class PortForwarderLoggerImpl implements PortForwarderLogger {
private final ResourceBundle messages;
private PortForwarderGui portForwarderGui;
/**
* Creates a new instance of PortForwarderLoggerImpl
*/
public PortForwarderLoggerImpl() {
messages = ResourceBundle.getBundle("Messages");
}
/**
* Tells the logger in which gui to log messages.
*
* @param portForwarderGui The gui to use
*/
public void setGui(PortForwarderGui portForwarderGui) {
this.portForwarderGui = portForwarderGui;
}
private String createTimeStamp() {
SimpleDateFormat dateFormat = new SimpleDateFormat("hh:mm:ss.SSS");
String timeStamp = dateFormat.format(new Date());
return timeStamp;
}
private String createMessage(String msg) {
return createTimeStamp() + " : " + msg;
}
public void log(final int logLevel, final int logCode,
final Object[] params, final Throwable throwable) {
if ((logLevel == PortForwarderConstants.LOG_LEVEL_ERROR) ||
(logLevel == PortForwarderConstants.LOG_LEVEL_INFO)) {
String msg =
```

```
MessageFormat.format(messages.getString("" + logCode),
params);
String messageString = createMessage(msg);
if (portForwarderGui == null) {
System.err.println("WARNING: Could not write to info area!");
System.err.println(messageString);
if (throwable != null) {
System.out.println(throwable.getMessage());
throwable.printStackTrace();
}
} else {
portForwarderGui.appendInfo(messageString +
System.getProperty("line.separator"));
if (throwable != null) {
portForwarderGui.appendInfo(throwable.getMessage() +
System.getProperty("line.separator"));
throwable.printStackTrace();
}
}
}
}
public void log(final int logLevel, final String msg,
final Throwable throwable) {
if (logLevel != PortForwarderConstants.LOG_LEVEL_DEBUG_VERBOSE) {
String messageString = createMessage(msg);
if (portForwarderGui == null) {
System.err.println("WARNING: Could not write to info area!");
System.err.println(messageString);
if (throwable != null) {
System.out.println(throwable.getMessage());
throwable.printStackTrace();
}
} else {
portForwarderGui.appendInfo(messageString +
System.getProperty("line.separator"));
if (throwable != null) {
portForwarderGui.appendInfo(throwable.getMessage() +
System.getProperty("line.separator"));
throwable.printStackTrace();
}
}
}
}
}
```

Connecting Through a Proxy

If the port forwarder is connecting through a proxy a number of properties need to be set for the port forwarder to know where and how to connect to the proxy.

The parameters are:

com.avaya.avg.portforwarder.http.proxyHost	The proxy host for HTTP & HTTPS accesses.

com.avaya.avg.portforwarder.http.proxyPort	The proxy port for HTTP & HTTPS accesses.
com.avaya.avg.portforwarder.http.proxyUserName	The proxy username for HTTP & HTTPS accesses.
com.avaya.avg.portforwarder.http.proxyPassword	The proxy password for HTTP & HTTPS accesses.

If the username and/or password is not set, the Port Forwarder API will call the **`PortForwarderAuthenticator.getProxyCredentials()`** function to obtain them.

Monitoring the Port Forwarder

The Port Forwarder uses the Observer/Observable framework, meaning that anyone wanting to have information from/about the Port Forwarder can add a Listener to it. Currently, you can monitor Port Forwarder status and statistics.

Note:

When using these features, it is important that the **`Observer.update()`** function does not block.

Status

Monitoring the Port Forwarder status gives you the ability to always know the state of the Port Forwarder, for example if it is ready to receive connections. Following is an example of the code for monitoring the status of the Port Forwarder.

```
private static class PortForwarderStatusListenerImpl
        implements PortForwarderStatusListener {
        public void statusChanged(int oldStatusCode, int newStatusCode) {
            statusNotifier.notifyObservers(new Integer(newStatusCode));
        }
    }

    private static class StatusObserver implements Observer {
        public void update(Observable observable, Object value) {
            portForwarderStatus = ((Integer) value).intValue();

            if (portForwarderStatus == PortForwarderConstants.
                                       PF_STATUS_INVALID_CREDENTIALS ||
               portForwarderStatus == PortForwarderConstants.PF_STATUS_STOPPED ||
              portForwarderStatus == PortForwarderConstants.PF_STATUS_GW_ERROR) {
                portForwarderGui.setStatusFailed();
            } else if (portForwarderStatus == PortForwarderConstants.
                                              PF_STATUS_INITIALIZING ||
                       portForwarderStatus == PortForwarderConstants.
                                              PF_STATUS_CONFIGURING) {
                portForwarderGui.setStatusInit();
            } else if (portForwarderStatus == PortForwarderConstants.
                                              PF_STATUS_LISTENERS_UP) {
                portForwarderGui.setStatusOk();
            }
        }
    }

    statusListener = new PortForwarderStatusListenerImpl();
    portForwarder.addStatusListener(statusListener);
```

Statistics

The Port Forwarder keeps track of all bytes passing through, allowing you to display or use the information in any way. An added statistics listener will receive a PortForwarderStatistics object either when a change has occurred or at a defined interval.

Following is an example of the code for monitoring Port Forwarder statistics.

```
    private static class StatisticsObserver implements Observer {
        public void update(Observable ob, Object value) {
            PortForwarderStatistics stats = (PortForwarderStatistics) value;
            System.out.println("Absolute     sent bytes: " +
                               stats.getAbsoluteSentBytes());
            System.out.println("             recv bytes: " +
                               stats.getAbsoluteReceivedBytes());
            System.out.println("             sent rate : " +
                               stats.getAbsoluteSentRate());
            System.out.println("             recv rate : " +
                               stats.getAbsoluteReceivedRate());
            System.out.println("Intermediate sent bytes: " +
                               stats.getIntermediateSentBytes());
            System.out.println("             recv bytes: " +
                               stats.getIntermediateReceivedBytes());
            System.out.println("             sent rate : " +
                               stats.getIntermediateSentRate());
            System.out.println("             recv rate : " +
                               stats.getIntermediateReceivedRate());
            System.out.println("Peak         sent rate : " +
                               stats.getPeakSentRate());
            System.out.println("             recv rate : " +
                               stats.getPeakReceivedRate());
        }
    }

    portForwarder.setStatisticsObserverInterval(3000);
    portForwarder.addStatisticsObserver(new StatisticsObserver());
```

This will print current statistics every 3 seconds.

Appendix Secure Portable Office Client

You can install the portable applications on the Secure Portable Office (SPO) client. Portable applications are the software programs that can be stored on any storage device like USB flash drive (generic or U3P format). Therefore, the user can add their favorite software applications like web browser, email client, office suite, calendar/scheduler, instant messaging client, antivirus, and so on a USB flash drive to be used on multiple computers.

SPO Release 9.0 in virtual mode supports the following software in Windows 32 bit and 64 bit platforms:

- Oracle Java Runtime Environment 1.7
- Microsoft Data Access 2.8
- Jet Database Endine 4.0
- Microsoft .Net Framework 3.5
- Avaya Contact Center Express Desktop 5.0
- Avaya One-X Agent 2.0
- Avaya 2050 IP Softphone 4.2

- Avaya customized Ceedo 4.x
- Net Direct x64 bit
- Microsoft IE9
- Mozilla FF 7.x

You can download portable applications into the USB flash drive from portable application websites like http://portableapps.com/, http://www.portablefreeware.com/, and http://www.u3.com/.

You can download Portable Applications to the USB flash drive in two ways:

- Public website
- AVG Server

Note:

Any user can download the portable application from the public server. But only authorized users can download the portable application on AVG server.

For information how to download the portable application from public server, see *Configuration - Secure Portable Office Client Guide* (NN46120-301).

Administrator SPO Client setup procedures

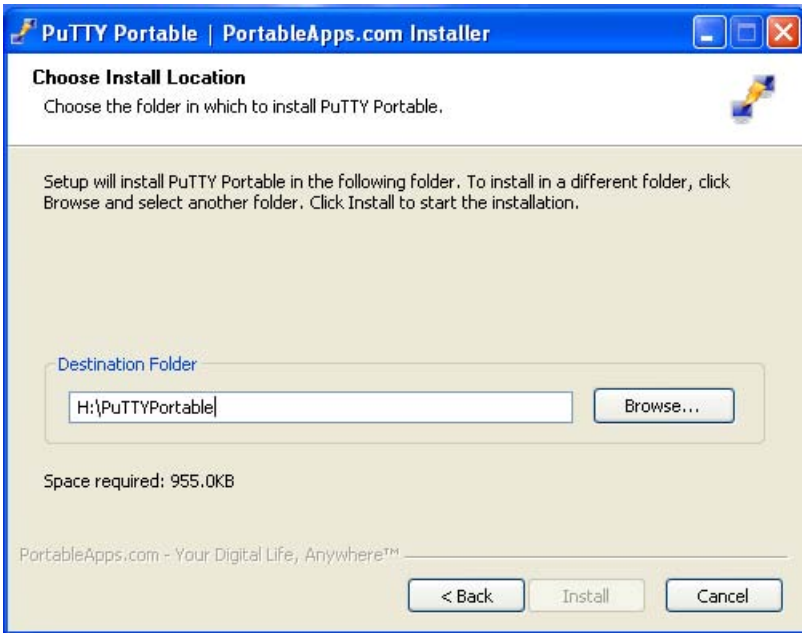
This section describes the steps for the authorised users to add the third party software to the AVG server:

Downloading portable applications on the desktop

The following procedure shows how to download the portable applications into the desktop.

1. Open web browser.
2. Type the IP addresshttp://www.portable.com/ to access the portable applications.
3. Download the putty file from http://portableapps.com/apps/intern%20et/putty_portable.
4. Click **Save** and save the file on the desktop.
5. Click **Run**.

6. Click **Next**.



7. Select the target location as remove-able disk and install the application.

8. Click **Finish**.

Uploading third party software into server

All the application software must be zipped before uploading it to the server. You can upload the zipped files either using CLI or BBI. Once the installation is complete go to the installed location using explorer and follow these steps:

1. Compress the directory using the WINZIP

   In this example, the zipped file is PuTTYPortable.zip.
2. Upload the compressed file into FTP/TFTP server.
3. Logon to the Avaya VPN Gateway using the CLI or BBI.
4. Add a new software using CLI or BBI:
   - If you are using CLI, type the command cfg/vpn<id>/spoclient/apps
   - If you are using CLI, navigate through VPN Gateways >> VPN <id> >> SPO >> Software Applications

For information on adding new software using CLI, see CLI Application Guide (NN46120-101).

For information on adding new software using BBI, see BBI Application Guide (NN46120-102).