Avaya VPN Gateway
BBI Application Guide

Avaya VPN Gateway

Release: **9.0**

Document Status: **Standard**

Document Number: **NN46120-102**

Document Version: **05.03**

Date: **August 2012**

Notices

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Licenses

Copyright

Third Party Components

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

Trademarks

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

Downloading documents

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

Contact Avaya Support

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

Contents

Customer service

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

Navigation

- "Getting technical documentation" on page 23
- "Getting product training" on page 23
- "Getting help from a distributor or reseller" on page 23
- "Getting technical support from the Avaya Web site" on page 24

Getting technical documentation

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

Getting product training

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

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

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

Preface

This guide provides examples to configure the Avaya VPN Gateway for VPN deployment by using the Browser-Based Management Interface (BBI). For configuration instructions based on the Command Line Interface (CLI), see the *Avaya CLI Application Guide for VPN*. For more information about the deployment of SSL acceleration, see the *Avaya Application Guide for SSL Acceleration (NN46120-100)*.

Who Should Use This Book

This guide is for network installers and system administrators who configure and maintain in a network. You must be familiar with Ethernet concepts and IP addressing. All IP addresses are examples and should not be used as is.

Related Documentation

For complete documentation to install, configure, and use the features of the Avaya VPN Gateway, see the following manuals:

- *Avaya VPN Gateway User's 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 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 SSL Acceleration through the CLI.
- *Avaya VPN Gateway CLI Application Guide for VPN* (NN46120-101)
  Provides examples on how to configure VPN deployment through the CLI.

- *Avaya VPN Gateway VPN Administrator Guide* (NN46120-105)
  VPN management guide intended for end-customers in a Secure Service Partitioning configuration.
- *Avaya VPN Gateway Release Notes* (NN46120-400)
  Lists new features available in version and provides up-to-date product information.
- *Avaya VPN Gateway Configuration - Secure Portable Office Client* (NN46120-301)

  Describes the configuration, installation, and authentication of the Secure Portable Office (SPO) client.
- *Avaya VPN Gateway Troubleshooting Guide* (NN46120-700)

  Describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway (AVG).
- *Avaya VPN Gateway VMware Getting Started Guide* (NN46120-302)

  Describes how to install, configure, and deploy the Avaya VPN Gateway VMware appliances.

  Other Avaya VPN Client related documents are:

  Avaya VPN Client - Installation and Upgrades (NN46110-412)

  Avaya VPN Client - Configuration (NN46110-509)

  Avaya VPN Client - Troubleshooting (NN46110-701)

Product Names

The software described in this manual runs on several hardware models. Whenever the generic terms *Avaya VPN Gateway, VPN Gateway* or *AVG* are used in the documentation, the following hardware models are implied:

- Avaya VPN Gateway 3050-VM (AVG 3050-VM)
- Avaya VPN Gateway 3070-VM (AVG 3070-VM)
- Avaya VPN Gateway 3090-VM (AVG 3090-VM)

How This Book is Organized

Chapter 1, “New in this release”. Introduces the new features for this release.

Chapter 2, “Getting Started”. Introduces how to enable BBI access in the CLI.

Chapter 3, “The Browser-Based Management Interface”. Introduces BBI, for example how to access the BBI, interface components, basic operation and a site map.

Chapter 4, “VPN Introduction”. Describes the main features of the Avaya VPN Gateway software.

Chapter 5, “Clientless Mode”. Describes how to setup a VPN for clientless mode, i.e. accessible with the available browser.

Chapter 6, “The Portal from an End-User Perspective”. Describes the Portal web page.

Chapter 7, “Net Direct”. Describes how to configure the system for use with the Net Direct client, a VPN client that can be temporarily downloaded for each Portal session.

Chapter 8, “Groups, Access Rules and Profiles”. Describes how to define user access groups with access rules and profiles.

Chapter 9, “Authentication Methods”. Describes how to configure a VPN to use external authentication servers (for example RADIUS), local database authentication or client certificate authentication.

Chapter 10, “Customize the Portal”. Describes how to customize the Portal, for example language version, logo, company name, colors, static texts and so on.

Chapter 11, “Group Links”. Describes how to define links on the Portal’s Home tab.

Chapter 12, “HTTP to HTTPS Redirection”. Describes how to configure the Avaya VPN Gateway for redirection of HTTP requests to HTTPS.

Chapter 13, “Secure Portable Office Client”. Describes how to configure Secure Portable Office (SPO).

Chapter 14, “Bandwidth Management. Describes how to configure bandwidth.

Chapter 15, “Configure Avaya Endpoint Access Control Agent”. Describes how to enable Avaya Endpoint Access Control Agent to check the client PC’s status.

Chapter 16, “WholeSecurity”. Describes how to enable a WholeSecurity scan of client PCs.

Chapter 17, “Secure Service Partitioning”. Describes how to configure hosting of multiple VPNs, a feature especially designed for Internet Service Providers (ISPs).

Chapter 18, "Branch Office Tunnels". Describes how to configure IPsec-based branch office tunnels.

Chapter 19, "Layer 2 Tunneling Protocol. Describes how to configure the Avaya VPN Gateway device for Layer 2 Tunneling Protocol (L2TP)

Chapter 20, "Network Access Protection. Describes howto configure the Network Access Protection (NAP) for Avaya VPN Gateway device.

Chapter 21, "Transparent Mode". Describes how to setup a VPN for transparent mode, i.e. accessible with the Avaya VPN Client.

Chapter 22, "Configure Portal Guard". Describes how to convert a regular HTTP site to generate HTTPS links.

Chapter 23, "SSL VPN Cluster Manager". Describes how to use the SSL VPN Cluster Manager for centralized software, configuration and user management for multiple clusters and/or clusters consisting of several Avaya VPN Gateways and VPNs

Appendix A, "Virtual Desktop". Describes how to access secure Web-based applications and services using virtual Desktop.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	This type is used for names of commands, files, and directories used within the text.	View the `readme.txt` file.
	It also depicts on-screen computer output and prompts.	`Main#`
`AaBbCc123`	This bold type appears in command examples. It shows text that must be typed in exactly as shown.	`Main#` **`sys`**
<AaBbCc123>	This italicized type appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	To establish a Telnet session, enter: `host#` **`telnet`** *<IP address>*
	This also shows book titles, special terms, or words to be emphasized.	Read your *User's Guide* thoroughly.
[ ]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	`host#` **`ls`** `[`**`-a`**`]`

CHAPTER 1
New in this release

The following sections detail what's new in *Avaya VPN Gateway Browser-Based Interface* (NN46120-102) for Release 9.0.

Navigation

- "Features" on page 31
- "Other changes" on page 33

Features

See the following sections for information about feature changes:

- "IPsec Two Factor authentication for Avaya VPN Gateway" on page 31.
- "Android L2TP/IPsec support" on page 32.
- "AES 256 support for IPsec" on page 32.
- "Secure Portable Office (SPO) support" on page 32
- "Feature support" on page 33

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 the following sections for more information on IPsec Two Factor authentication:

- "Accessing the Portal Web Page" on page 105.
- "Secondary and Two Factor authentication" on page 240.
- "Configure Advanced settings" on page 348.

Android L2TP/IPsec support

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 compatibility matrix in *AVG 9.0 Release Notes* (NN46120-400).

Refer to the following procedures when configuring L2TP connections for the Android client:

- "Configuring L2TP connections for Android" on page 585.

AES 256 support for IPsec

Release 9.0 adds AES 256 support for IPsec.

Refer to the following sections for AES 256 support for IPsec:

- "Configuring Authentication and Encryption" on page 567.
- "Configuring Diffie-Hellman Groups" on page 569.

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 in the Ceedo environment. The following host resources are blocked inside Ceedo:

- Access to network shares and drives

- Access to printing
- Drag and drop
- Clipboard access

Refer to the following section for configuring the Secure Portable Office (SPO) client:

- “Secure Portable Office Client” on page 431.

Feature support

- Release 9.0 upgrades Java RDP 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.
- Release 9.0 supports Net Direct Mac OS X 10.7 (Lion).

Other changes

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

- Added the section, “Configure Advanced settings” on page 348.
- Added the section, “Create a Linkset for Windows Terminal Server” on page 404.
- Added the section, “Enable Avaya VPN Client (SSL)” on page 631.
- Updated step 23, with WTS parameters in “Example 7b: Windows Terminal Server Port Forwarder Link with Automatic Portal Login” on page 410.
- Renamed TunnelGuard to Avaya Endpoint Access Control Agent.
- Moved “Virtual Desktop” to Appendix A, “Virtual Desktop” on page 689.
- Added Avaya VPN Gateway 3090-VM to Hardware list, “Hardware Limits” on page 77.
- Added a table for Avaya VPN Client authentication types, “Avaya VPN Client authentication types” on page 242.

CHAPTER 2

Getting Started

This chapter describes the software features and requirements for the Browser-Based Management Interface (BBI) and explains how to access the BBI start page.

Features

You can access virtually all Avaya VPN Gateway configuration and monitoring functions through the BBI, a Web-based management interface for the Avaya VPN Gateway software. The BBI has the following features.

- most of the configuration and monitoring functions of the Command Line Interface (CLI)
- intuitive, easy-to-use interface structure
- nothing to install; the BBI is part of the Avaya VPN Gateway software
- can be upgraded as future software releases are available
- can be accessed using HTTP, or secure HTTPS
- up to 10 simultaneous BBI sessions

Minimum Setup

To access the BBI, a minimum configuration is required on your Avaya VPN Gateway.

Setup for VPN Gateways

After you perform the Initial Setup procedure for your model (see the "Initial Setup" chapter in your *VPN Gateway User's Guide*), some additional configuration is required in the CLI to permit BBI access.

NOTE – Make sure that the host IP address and the management IP address (MIP) that you entered during the Initial Setup are accessible to your browser host network.

1. **Enable the BBI.**

By default, the BBI is disabled for HTTP and HTTPS access. You can enable the BBI for HTTP and/or HTTPS.

NOTE – HTTP is not a secure protocol. All data (including passwords) between an HTTP client and the Avaya VPN Gateway is unencrypted and is subject only to weak authentication. If secure remote access is required, consider using HTTPS instead of HTTP.

To allow remote BBI access, enter the following commands in the CLI.

- Enable HTTP access and set the HTTP logical port:

```
>> Main# /cfg/sys/adm/http/ena              HTTP access enabled
>> Main# /cfg/sys/adm/http/port 80          HTTP port set to 80 (default)
```

NOTE – The default HTTP port value is well-known HTTP port 80. If you change this value (for example, to 81), users must append the port value to the host IP address (for example, http://10.10.1.110:81) when opening a connection to the Avaya VPN Gateway or SSL Processor. If you set up HTTP to HTTPS redirection during the initial setup procedure, port 80 is occupied. Specify another port number (for example 81) for BBI access through HTTP.

- Enable HTTPS access:

```
>> Main# /cfg/sys/adm/https/ena             HTTPS access enabled
>> Main# /cfg/sys/adm/https/port 1025       HTTPS port set to 1025
```

You can choose any port for BBI traffic, except one that other traffic on your system uses (the CLI, in fact, rejects the selection of ports that are known to bear traffic).

2. **Add your browser host’s network address to the access list:**

```
>> Main# /cfg/sys/adm/accesslist/add <network IP address>
```

This step is optional. If the list is empty, there is no access restrictions based on the client network IP address.

NOTE – If you add your browser host’s network to the Access list, you must also add the Management IP address and the Interface 1 IP addresses of existing Avaya VPN Gateways in the cluster to the Access list (or a network that covers all of these IP addresses). Otherwise, the Avaya VPN Gateways cannot communicate.

3. **Apply the changes.**

```
>> Main# apply
```

CHAPTER 3

The Browser-Based Management Interface

This chapter provides a general introduction the BBI, for example global commands, general site navigation, and on-line help. For configuration examples, see chapters 3-18.

For detailed information about the fields and list boxes available on the BBI pages, refer to the *VPN Gateway Command Reference* (see “Related Documentation” on page 25).

Web Browser Setup

Once you have configured your system for Web access, you can connect to the BBI through a properly configured Web browser.

To display the BBI, your browser must be configured to work with frames and JavaScript. Both the Netscape and Internet Explorer browsers that have been verified to work with the BBI, are default-configured to work with frames and JavaScript, and require no additional setup. However, you should check your Web browser’s features and configuration to make sure frames and JavaScript are enabled.

NOTE – JavaScript is not the same as Java. Please make sure that JavaScript is enabled in your Web browser.

Host Setup

Refer to “Minimum Setup” on page 36 or to the user documentation for your host (Avaya VPN Gateway or SSL Processor) for configuring web access on your system (see “Related Documentation” on page 25).

Starting the BBI

Once you have completed the necessary setup procedures, follow these steps to launch the BBI:

1. **Start your Web browser.**

2a. **For http connections, enter http://**<*host IP* or *MIP address* or *DNS name of your AVG*> **in the Web browser URL field.**

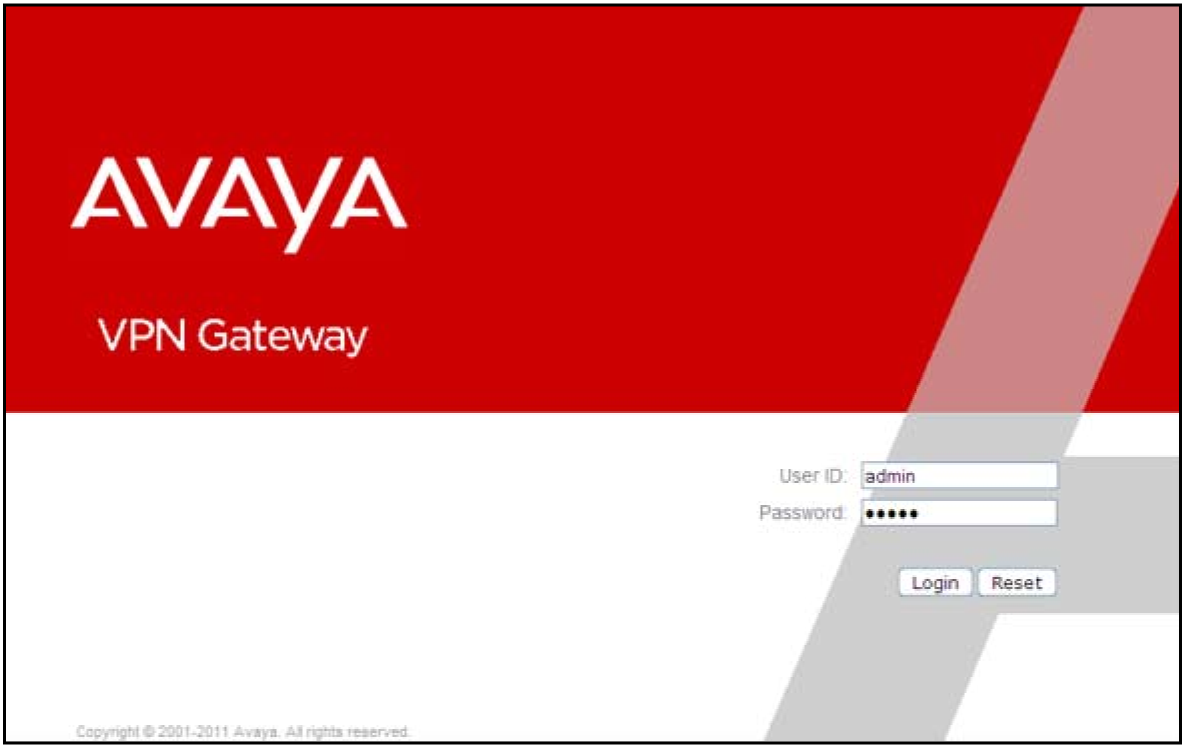
For example, if your host IP address is 200.200.200.100, you would enter the following in your browser: http://200.200.200.100

2b. **If the host name (for example, AVG_3050_lab) for 200.200.200.100 has been added to your local domain name server, you could enter it instead.**

2c. **For https connections, enter https://**<*host MIP address*>**:**<*port number*> **in the browser URL field.**

3. **Log in to the Avaya VPN Gateway or SSL Processor.**

   Proper host configuration includes a host IP that is accessible to your browser network. If your host and browser are properly configured, the Login page is displayed:



User ID: admin

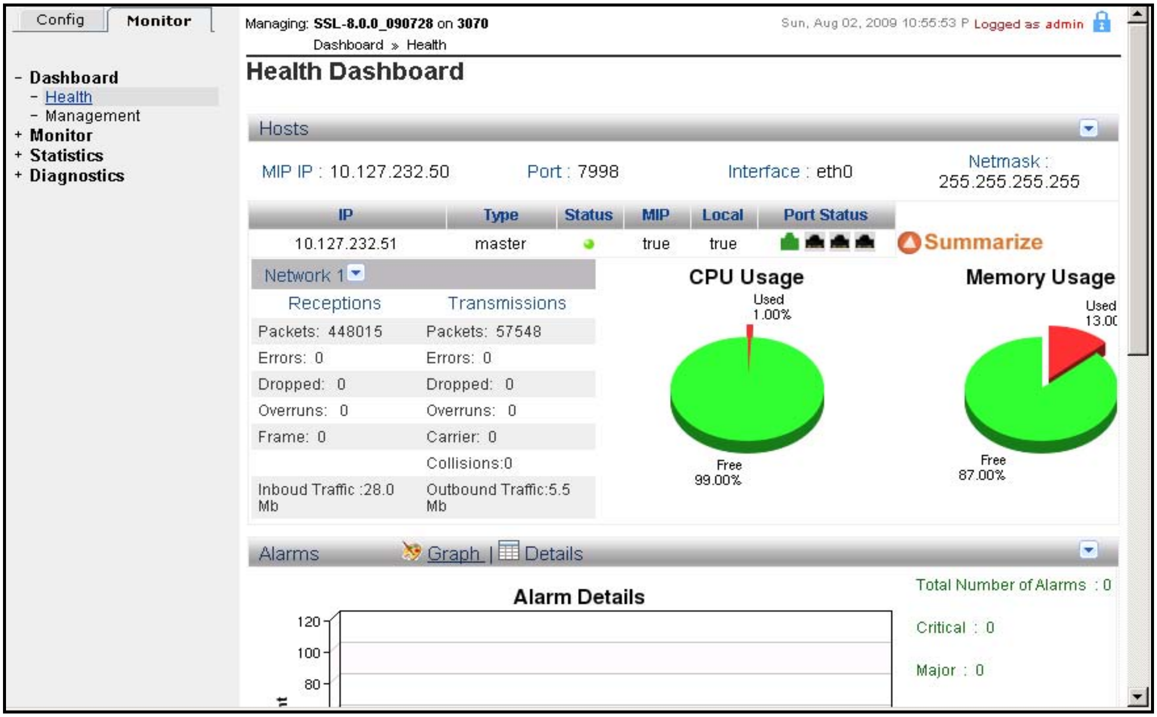
Password: •••••

4. **Enter the account name and password for the host's administrator or user account.**

   For more password information, see the *VPN Gateway Command Reference*.

5. **Click the Login button or press ENTER.**

   When the proper account name and password combination is entered, the wizards page (the first page in the BBI) is displayed in your browser's viewing area (see next page).



Managing: **SSL-8.0.0_090728** on **3070**

Sun, Aug 02, 2009 10:55:53 P Logged as admin

Health Dashboard

Hosts

MIP IP : 10.127.232.50   Port : 7998   Interface : eth0   Netmask : 255.255.255.255

IP	Type	Status	MIP	Local	Port Status
10.127.232.51	master	●	true	true	

Network 1

Receptions	Transmissions
Packets: 448015	Packets: 57548
Errors: 0	Errors: 0
Dropped: 0	Dropped: 0
Overruns: 0	Overruns: 0
Frame: 0	Carrier: 0
	Collisions:0
Inboud Traffic :28.0 Mb	Outbound Traffic:5.5 Mb

CPU Usage: Used 1.00%, Free 99.00%

Memory Usage: Used 13.0(, Free 87.00%

Alarms

Total Number of Alarms : 0

Critical : 0

Major : 0

GUI Lock

The GUI lock warning message displayed at the top of the screen is only displayed just after login. If you switch to another BBI screen without taking the GUI lock, the message will disappear.

On the GUI Lock page (click the **Go to 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 Avaya VPN Gateway configuration through the BBI. The padlock symbol top right changes from blue to green. 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. For these users, the padlock symbol is red.

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

If necessary, it is possible to take the lock from an operator that currently has the lock. This is done in the same way as when taking the lock the first time.

NOTE – Changes made by another operator through the CLI is possible even if the GUI lock is activated.

VPN Lock

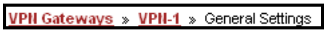
The ability to lock a specific VPN is only available if a Secure Service Partitioning license is loaded (see Chapter 17, “Secure Service Partitioning).

Global Administrators

The VPN lock lets you (as the global administrator) lock a specific VPN, for example to notify other administrators that the VPN is currently being edited. You can however apply configuration changes even if a VPN lock is owned by somebody else. You will not be able to apply changes if a GUI lock has been taken by another administrator.

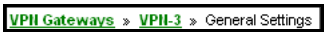
The padlock symbol in the BBI header does not indicate whether or not a VPN lock is taken. This is instead indicated with the color of the breadcrumbs for VPN related pages:

Brown color of the bread crumb indicates that no VPN lock has been taken.



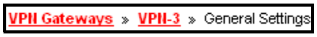
VPN Gateways » VPN-1 » General Settings

Green color of the bread crumb indicates that you currently have the lock.



VPN Gateways » VPN-3 » General Settings

Red color of the bread crumb indicates that another administrator has the lock.



VPN Gateways » VPN-3 » General Settings

By clicking the padlock icon, the **VPN Gateways>VPN #>VPN Lock** page is displayed. Global administrators can also view VPN Lock information about the **VPN Gateways** and **Monitor>GUI Lock** pages.

VPN Administrators

The VPN lock lets the VPN administrator of a specific VPN lock the VPN. While the VPN is locked by that administrator, no other VPN administrator of that VPN can apply configuration changes. VPN administrators will not be able to apply changes if a GUI lock has been taken by a global administrator, even if they own the VPN lock.

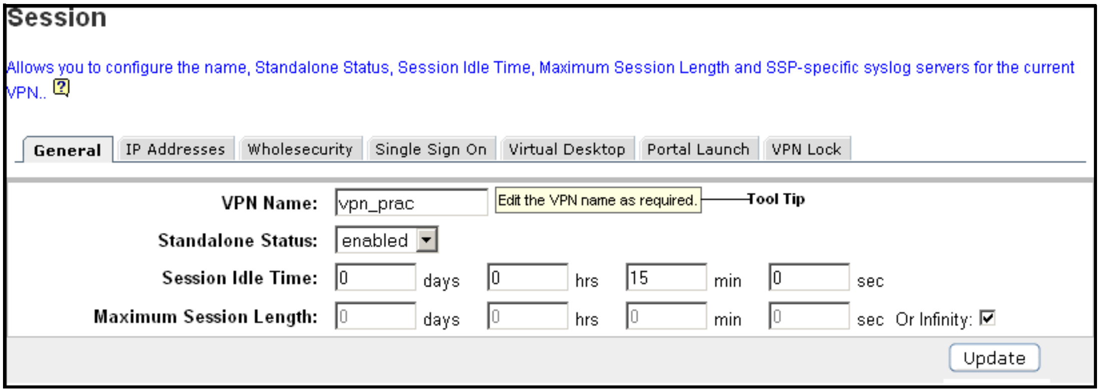
To lock or release the lock, or to view who currently has the lock, the VPN administrator should go to the **VPN Gateways>VPN #>VPN Lock** or the **Monitor>GUI Lock** page.

Active Alarms

If there are active alarms, this is displayed with the text **“Notice: There are active alarms”**. To view active alarms (if any), click the **Go To Alarms Page** button.

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 filed is displayed in the tool tip.



Session

Allows you to configure the name, Standalone Status, Session Idle Time, Maximum Session Length and SSP-specific syslog servers for the current VPN..

VPN Name: vpn_prac

Edit the VPN name as required.

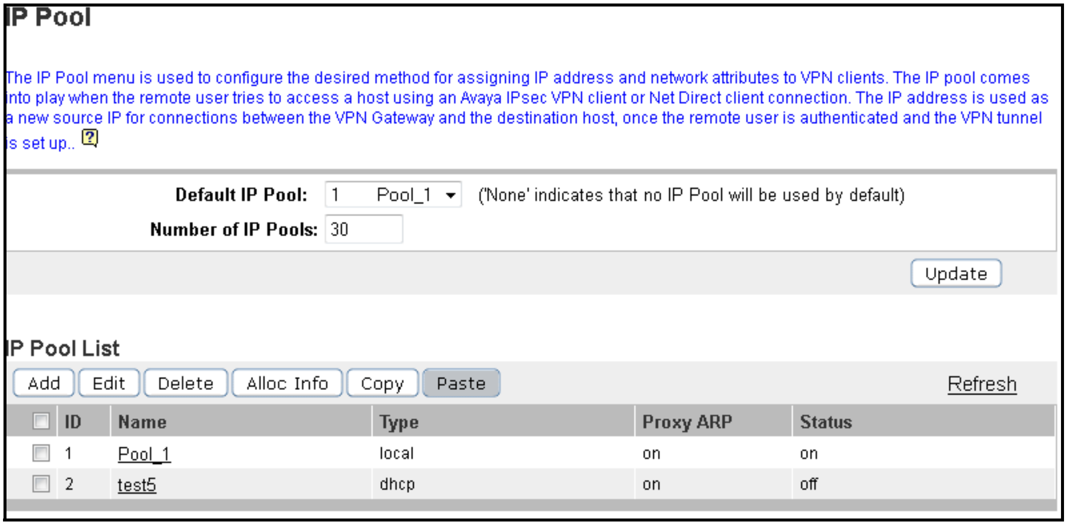
Standalone Status: enabled

Session Idle Time: 0 days 0 hrs 15 min 0 sec

Maximum Session Length: 0 days 0 hrs 0 min 0 sec Or Infinity: ☑

Copy and Paste

You can do copy and paste of IP Pools, Groups, Authentication servers, SSL Offload servers, IPSec's, IKE, User and BO Tunnel and Portal Linksets between VPNs that are supported in the respective tables using “Copy” and “Paste” buttons.



IP Pool

The IP Pool menu is used to configure the desired method for assigning IP address and network attributes to VPN clients. The IP pool comes into play when the remote user tries to access a host using an Avaya IPsec VPN client or Net Direct client connection. The IP address is used as a new source IP for connections between the VPN Gateway and the destination host, once the remote user is authenticated and the VPN tunnel is set up..

Default IP Pool: 1 Pool_1 ('None' indicates that no IP Pool will be used by default)

Number of IP Pools: 30

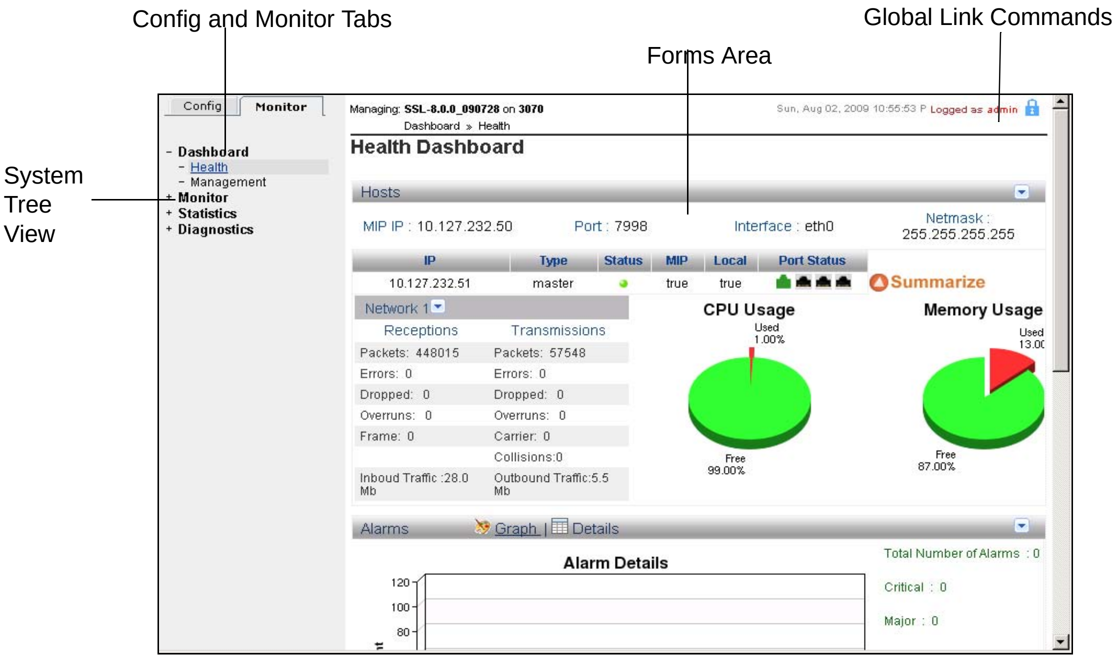
IP Pool List

□	ID	Name	Type	Proxy ARP	Status
□	1	Pool_1	local	on	on
□	2	test5	dhcp	on	off

For Example, if a IP Pool’s configuration has to be copied from VPN 1 and pasted to VPN 2. Select VPN 1 from the VPN table and navigate to IP Pool table page and check the IP Pool from the IP Pool List table that has to be copied and click on the Copy button. Now, select VPN 2 and Navigate IP Pool page and click on the Paste button.

Basics of the Browser-Based Interface

Once you are properly logged in, the Avaya VPN Gateway Browser- Based Interface (BBI) appears in your Web browser's viewing window:



Managing: **SSL-8.0.0_090728** on **3070**

Sun, Aug 02, 2009 10:55:53 P Logged as admin

Dashboard » Health

Health Dashboard

Hosts

MIP IP : 10.127.232.50   Port : 7998   Interface : eth0   Netmask : 255.255.255.255

IP	Type	Status	MIP	Local	Port Status
10.127.232.51	master	●	true	true	

Network 1

Receptions	Transmissions
Packets: 448015	Packets: 57548
Errors: 0	Errors: 0
Dropped: 0	Dropped: 0
Overruns: 0	Overruns: 0
Frame: 0	Carrier: 0
	Collisions:0
Inboud Traffic :28.0 Mb	Outbound Traffic:5.5 Mb

Total Number of Alarms : 0

Critical : 0

Major : 0

Following are the main regions on the screen:

- System tree view
- Config and Monitor tabs
- Forms area
- Global link commands

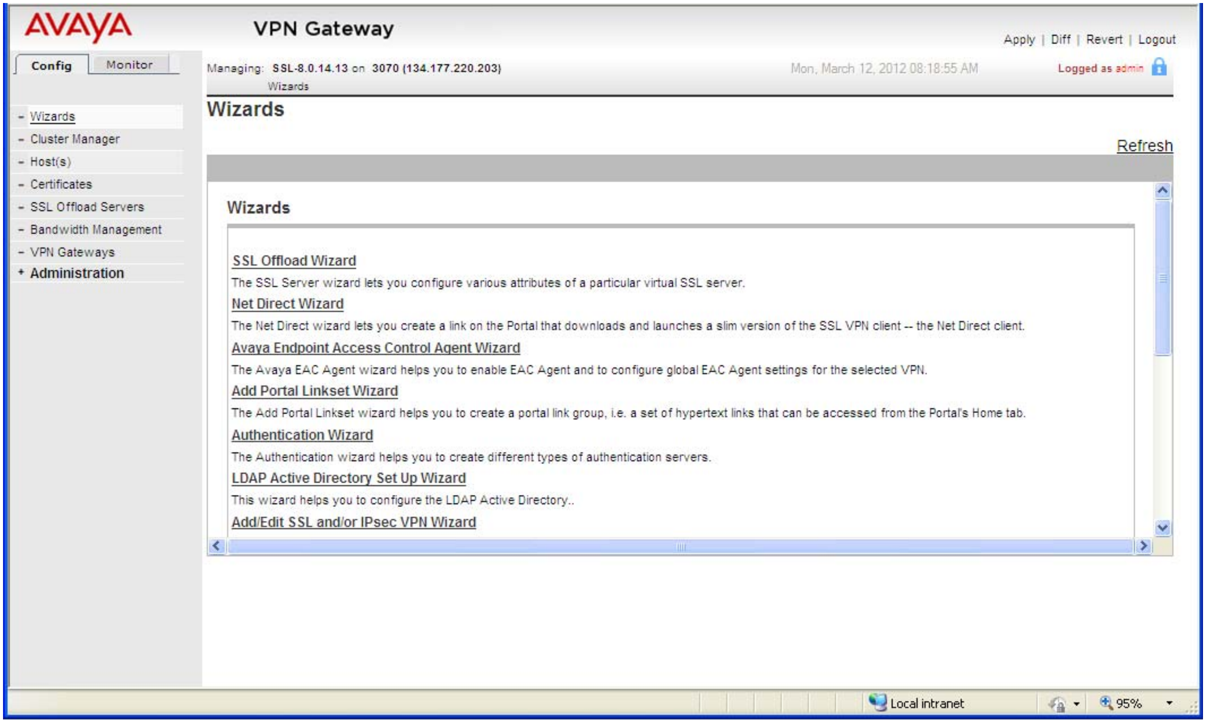
System tree view

The System Tree View consists of items (Cluster, Network 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 are displayed. Several items can be expanded at the same time, which gives you a good overview when configuring the system.

Note that some of the +-marked items (for example Certificates and VPN Gateways) display information when selected, i.e. besides showing sub-items.

Config

The Config tab lets you configure various VPN options.



SSL Offload Wizard

The SSL Server wizard lets you configure various attributes of a particular virtual SSL server.

Net Direct Wizard

The Net Direct wizard lets you create a link on the Portal that downloads and launches a slim version of the SSL VPN client -- the Net Direct client.

Avaya Endpoint Access Control Agent Wizard

The Avaya EAC Agent wizard helps you to enable EAC Agent and to configure global EAC Agent settings for the selected VPN.

Add Portal Linkset Wizard

The Add Portal Linkset wizard helps you to create a portal link group, i.e. a set of hypertext links that can be accessed from the Portal's Home tab.

Authentication Wizard

The Authentication wizard helps you to create different types of authentication servers.

LDAP Active Directory Set Up Wizard

This wizard helps you to configure the LDAP Active Directory..

Add/Edit SSL and/or IPsec VPN Wizard

- ***Wizards*** **-** All wizard pages contains Back (except in the first page), Next (except in the last page), and Cancel buttons. Intermediate 'Finish' button completes the minimal configuration. This button is enabled once the user has completed configuring the mandatory parameters. By this, the user can skip the configuration of optional fields. This makes the feature to work on minimal settings. Default values are provided in the fields wherever it is applicable.

Following wizards are available for configuration of different applications of the VPN Gateway.

- SSL offload: The SSL Server wizard lets you configure various attributes of a particular virtual SSL server.
- Net Direct: The Net Direct wizard lets you create a link on the Portal that downloads and launches a slim version of the Avaya VPN Client -- the Net Direct client.

  - Avaya Endpoint Access Control Agent: The Avaya EAC Agent wizard helps you to enable EAC Agent and to configure global EAC Agent settings for the selected VPN.
  - Add Portal Linkset: The Add Portal Linkset wizard helps you to create a portal link group, that is a set of hypertext links that can be accessed from the Portal's Home tab.
  - Authentication: The Authentication wizard helps you to create different types of authentication servers.
  - LDAP Active Directory Setup: This wizard helps you to configure the LDAP Active Directory.
  - Add/Edit SSL and/or IPsec VPN: The Add/Edit SSL and/or IPsec VPN wizard helps you to configure SSL-VPN and/or to configure the VPN Gateway to support IPsec-based user tunnels and branch office tunnels.
  - Certificate: The Certificate wizard helps you to manage private keys and certificates.
  - IPsec: The IPsec wizard used to configure the VPN Gateway to support IPsec-based user tunnels and branch office tunnels.
  - L2TP: The L2TP wizard used to configure the VPN Gateway to support L2TP-based user tunnels.
  - Manage Portal: The Manage wizard helps you to customize the look and behavior of Portal web page.
  - Manage Administrative Access to AVG: The Manage Administrative Access to AVG Wizard helps you configure the Administrative Settings of AVG.
  - User Group: User Group Wizard help to configure user access groups for mobile users.

NOTE – Mandatory fields are marked with '*'

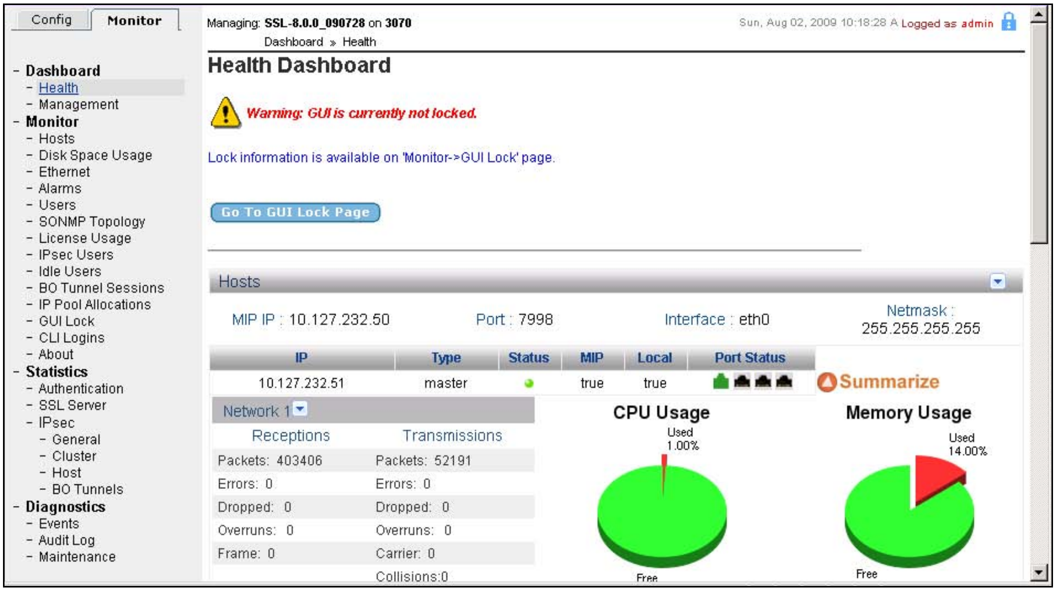
- ***Cluster Manager*** - SSL-VPN Cluster Manager is a Java-based application that works as a minimum administering tool that is the user is able to configure some of the options available in the BBI or CLI by providing status update as well as configuration of VPN Gateway devices.
- ***Host(s)*** - Allows you to set the Management IP(MIP) address and configure the VPN Gateway(s) to either master or slave. You can also halt, reboot or delete a VPN Gateway remotely.
- ***Certificates*** - Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway.
- ***SSL Offload Servers*** - Allows you to configure virtual SSL servers.

- ***Bandwidth Management* -** Allows you to allocate bandwidth for each user based on the users group membership. The user types can be Net Direct Installable Client (NDIC), Portal, and IPSec Client.
- ***VPN Gateways* -** Lists the configured VPN(s) and also allows you to add, edit and delete VPN(s).
- ***Administration* -** Following options are available under Administration:
  - ***Operation*** - Operation allows you to:
    - halt, reboot, or delete the configuration of the selected Avaya VPN Gateway(s).
    - save current configuration including private keys and certificates to the local system.
    - download software upgrade packages from local system.
    - manage language definition files.
  - ***System* -** Allows you to set the system date, time and time zone, add NTP and global DNS servers, configure syslog servers, disable tracing, and manage static routes.
  - ***Users* -** The User menu is used to change the password for the currently logged in administrator user, add a new administrator user account, or delete an existing administrator user account. By using the edit menu option, you can also change the password and group assignment for a specified user account. Only users with Administrator rights can add or delete user accounts, or change the password of another user account.
  - ***Remote Access* -** Allows you to enable/disable Telnet and SSH access, and HTTP/ HTTPS access.
  - ***Access list* -** The Access List menu is used for controlling Telnet and SSH access to the AVG host. The access control rules can be applied to individual machines, or to all machines on a specific network.
  - ***SSH Keys* -** The SSH Keys menu is used to generate new SSH host keys for the cluster. It also lets you display the current host keys and manage known host keys, for example paste or import SSH keys from known remote hosts.
  - ***SNMP* -** SNMP menu is used for configuring network management of your VPN Gateways. SNMP (Simple Network Management Protocol) is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant agents on the VPN Gateways store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

- ***IPPool*** - Lets you enable/disable the feature to use more than the default number of IP Pools for the current VPN.
- ***SONMP*** **-** Configure SynOptics Network Management Protocol (SONMP). When SONMP is enabled, VPN Gateways in the cluster exchange multicast packets. The IP address of an iSD is written into the hello packets. The topology table can be viewed from 'Monitor->SONMP Topology' page under the 'Monitor' tab.
- ***RADIUS*** **-** RADIUS menu is used to configure RADIUS authentication of system users (device administrator). Authentication applies to both CLI and WebUI users.
- ***RSA Server*** **-** The RSA Servers menu lets you configure the symbolic name for the RSA server and import the sdconf.rec configuration file.
- ***Auditing*** **-** The Audit menu is used to configure a RADIUS server to receive log messages about commands executed in the CLI and operations done in the WebUI. If auditing is enabled but no RADIUS server is configured, events will still be generated to the event log and any configured syslog servers.
- ***In-Memory*** **-** The In-Memory menu is used to configure status of the internal memory & to set the size of the internal buffer.

Monitor

The Monitor tab lets you view and monitor various VPN configured options:



Managing: **SSL-8.0.0_090728** on **3070**

Sun, Aug 02, 2009 10:18:28 A Logged as admin

Dashboard » Health

Health Dashboard

Warning: GUI is currently not locked.

Lock information is available on 'Monitor->GUI Lock' page.

MIP IP : 10.127.232.50 Port : 7998 Interface : eth0 Netmask : 255.255.255.255

IP	Type	Status	MIP	Local	Port Status
10.127.232.51	master	●	true	true	

Receptions	Transmissions
Packets: 403406	Packets: 52191
Errors: 0	Errors: 0
Dropped: 0	Dropped: 0
Overruns: 0	Overruns: 0
Frame: 0	Carrier: 0
	Collisions:0

- ***Dashboard* -** This displays health and management data collated from device. Following options are available under Dashboard:
  - □ ***Health***- Displays device health, compliancy, and audit details.
  - □ ***Management***- Displays general information about device settings, log details, different type of users grouped into specific categories, and license usage.
- ***Monitor* -** This displays status of all the interfaces. Following options are available under Monitor:
  - □ ***Hosts***- Displays the IP addresses, master/slave assignments, CPU usage, memory usage and operational status and so on. for all the VPN Gateways in the cluster.
  - □ ***Disk Space Usage***- Displays the amount of disk space available on all the currently mounted filesystems. Disk space is shown in 1K blocks by default.
  - □ ***Ethernet* -** Displays statistics for the Ethernet Network Interface Card (NIC) on the particular Avaya VPN Gateway host to which you have connected.
  - □ ***Alarms* -** Displays all active alarms by their main attributes: severity level, alarm ID number, date and time when triggered, alarm name, sender and cause.
  - □ ***Users*** - Provides information about the users currently logged into the system.
  - □ ***SONMP Topology* -** Provides SONMP topology information.
  - □ ***License Usage***- Displays logged in VPN users (under Used) and allowed number of concurrent VPN users in the cluster (under Size). The number is presented for each license type (i.e. SSL and IPsec) and - if the Secure Service Partitioning feature is used - for each VPN.
  - □ ***IPsec Users* -** Provides information about the current IPsec sessions.
  - □ ***Idle Users* -** Provides information about the idle SSL-VPN Portal users currently logged into the system.
  - □ ***BO Tunnel sessions* -** Provides information about the current active Branch Office Tunnel sessions.
  - □ ***IP Pool Allocations* -** Provides IP Pool information per IP pool and VPN.
  - □ ***GUI Lock*** - Provides information about the GUI and VPN lock status.
  - □ ***CLI Logins*** - Provides information about CLI user(s) login.
  - □ ***About*** - Provides general information about the system, like product and version number.

- Statistics - Following options are available under Statistics:
  - ***Authentication* -** Displays the total authentication statistics for all VPN Gateways in the cluster because the system was started.
  - ***SSL server* -** Displays the SSL statistics.
  - ***IPsec* -** Following options are available under IPsec:
    - General - Displays the IP Statistics.
    - Cluster - Displays the Cluster statistics.
    - Host - Displays the hosts statistics.
    - BO Tunnels - Displays the number of encoded and decoded kBytes per second during the last minute, for branch office tunnels in all VPNs in the cluster.
  - ***Bandwidth Management* -** Displays information related to the Bandwidth management.
- ***Diagnostics* -** Following options are available under Diagnostics:
  - Events - Displays the most recent 64k of the event log file existing on the selected host.
  - Audit Log - Displays the most recent 64k of the audit log file existing on the selected host.
  - Maintenance - This lets you to do the following:
    - check the configuration
    - log certain information pertaining to a VPN user session
    - start logging of events to an internal buffer, stop logging, clear the Internal log and to display the last **n** messages. **n** is the multiples of 10 and is calculated from the Buffer Size value configured in Administration > In-Memory page in **Config** tab.
    - collect Dump logs and statistics.

Forms Area

The Forms area displays information about the options available in the system tree view. Using this you can specify information required for system configuration.

Global Command Links

These command 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 the Avaya VPN Gateway software in the following manner. To access the full functionality of the BBI, you must be logged in as administrator:

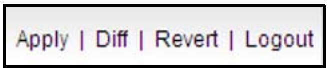
- Select from a series of pages and sub-pages, and modify fields to create the desired configuration.
- When finished making changes on any given page, submit the form using the appropriate **Update** buttons. If you select a new form or end the session without submitting the information, the changes 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 CLI or BBI administrator sessions are open at the same time, only pending changes made during your current session are affected by the Diff, Revert, or Logout commands. However, if multiple CLI or 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. CLI changes are still possible.

Global Command Forms

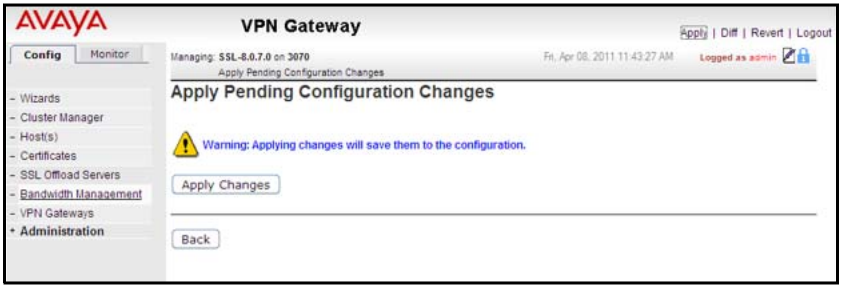
The global command links are always available at the top of each form:



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, and for saving the configurations change and putting them into effect.



Managing: SSL-8.0.7.0 on 3070

Fri, Apr 08, 2011 11:43:27 AM

Logged as admin

Apply Pending Configuration Changes

Apply Pending Configuration Changes

Warning: Applying changes will save them to the configuration.

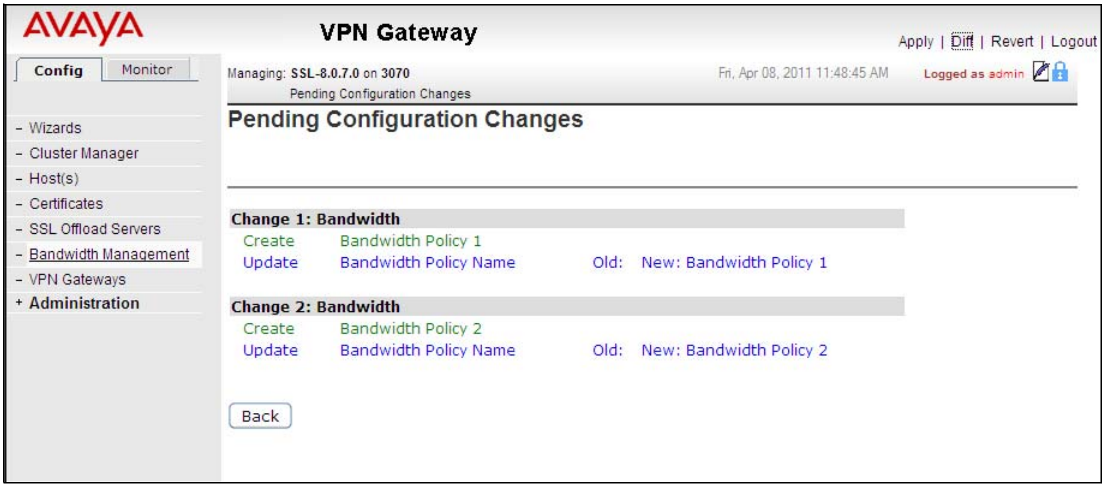
The Global Apply form includes the following items:

- 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.



Pending Configuration Changes

Change 1: Bandwidth

Create	Bandwidth Policy 1		
Update	Bandwidth Policy Name	Old:	New: Bandwidth Policy 1

Change 2: Bandwidth

Create	Bandwidth Policy 2		
Update	Bandwidth Policy Name	Old:	New: Bandwidth Policy 2

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:

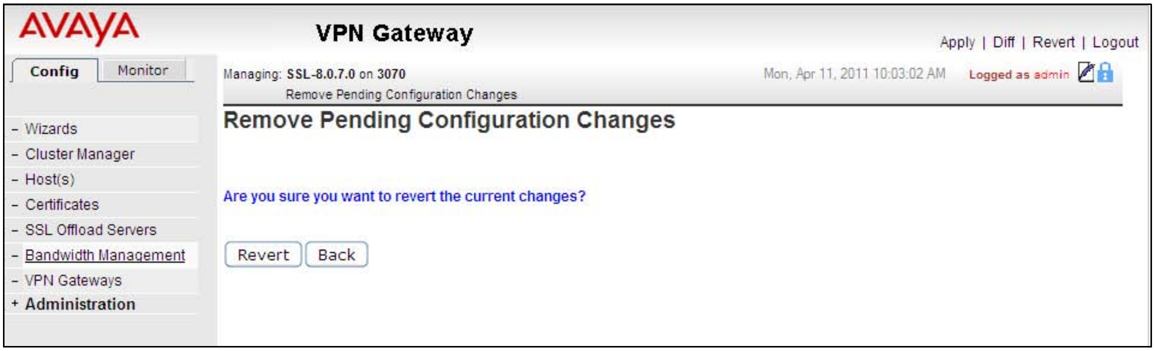
- Green: New items that are *added* to the configuration when the global Apply command is given and verified.
- Blue: Existing items that are *modified*.
- Red: Configuration items that are *deleted*.

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.



Managing: SSL-8.0.7.0 on 3070

Mon, Apr 11, 2011 10:03:02 AM

Logged as admin

Remove Pending Configuration Changes

Remove Pending Configuration Changes

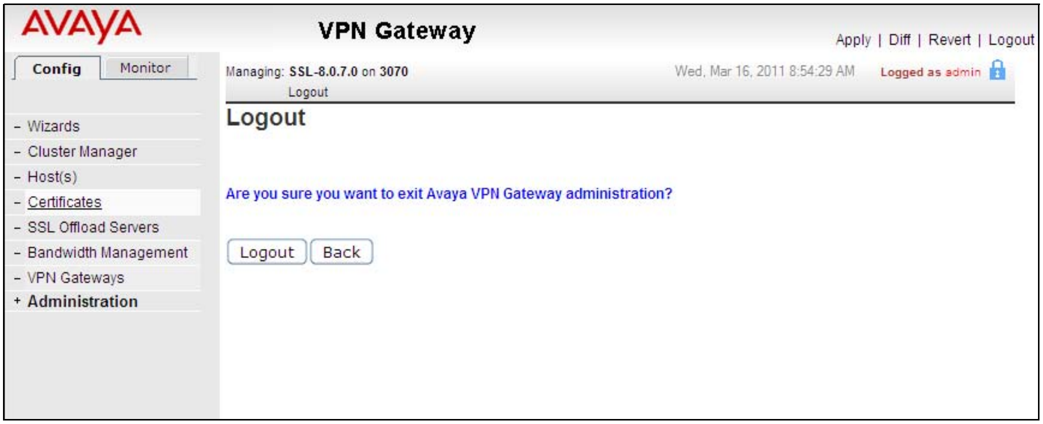
Are you sure you want to revert the current changes?

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 cancelling pending changes.

Logout

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



Are you sure you want to exit Avaya VPN Gateway administration?

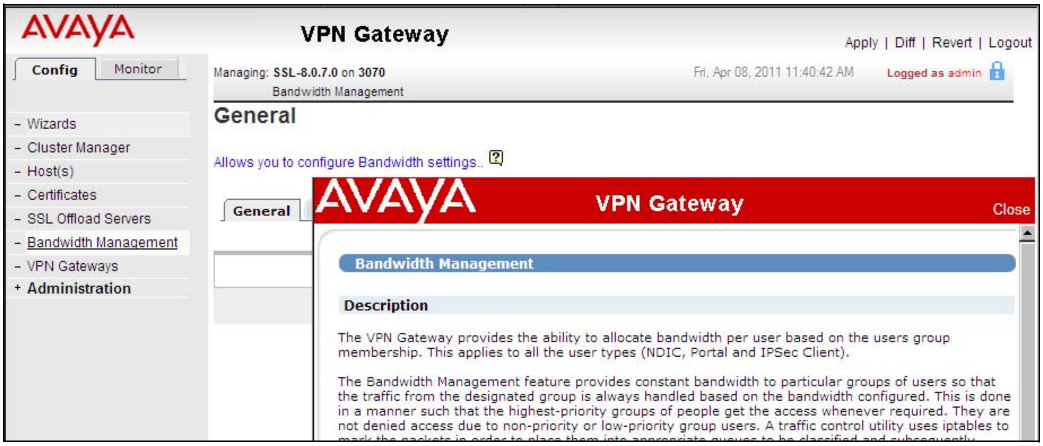
This form includes the following items:

- Logout button. This button terminates the current user session. Any configuration changes made during this session that have not yet been applied are 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 button provides assistance with forms in the BBI. The help button is available in every page of the GUI. The help is context-sensitive, which means that the help page displays detailed information about the form that is presently displayed.



The VPN Gateway provides the ability to allocate bandwidth per user based on the users group membership. This applies to all the user types (NDIC, Portal and IPSec Client).

The Bandwidth Management feature provides constant bandwidth to particular groups of users so that the traffic from the designated group is always handled based on the bandwidth configured. This is done in a manner such that the highest-priority groups of people get the access whenever required. They are not denied access due to non-priority or low-priority group users. A traffic control utility uses iptables to

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

The help window consists of the ***Close*** (top right corner) option to close the help window.

Site Map

The Site Map table provides the list of sub-page menus and status/command labels for each form to aid navigation through the BBI. Items in parenthesis are for clarification or to indicate the operations that can be performed.

Table 3-1 BBI site map

Folder	Sub Folder/Page	Page	Status and Command Labels
Wizards			SSL Offload, Net Direct, Avaya Endpoint Access Control Agent, Add Portal linkset, Authentication, LDAP Active Directory Set Up, Add/Edit SSL and/or IPsec VPN, Certificate, IPsec, L2TP, Manage portal, Manage Administrative access to AVG, User Group, and SSP VPN.
Cluster Manager			Launch SSL-VPN Cluster Manager, a Java-based application for centralized cluster management.
Hosts			Management IP(MIP) Address and SSL VPN Host(s)
Certificates			
	General	Certificate Information	Certificate Information Table, Certificate Update Page, and Certificate Show Page
	Import	Import Certificate and/or Key as File	Import File and Import Text
	Export	Export Certificate and/or Key to File	Export File and Export Text
	Generate	Generate Signing Request	Request, Signed Certificates, and Test Certificates.
	Sign Request	Sign Request	Certificate Information, Signed Certificate, Certificate Signing Request.
	Revocation List	Revocation List	General and Automatic CRL.

Folder	Sub Folder/Page	Page	Status and Command Labels
SSL Offload Servers			General, HTTP Type, Socks Type, Trace, Advanced, Load Balancing
Bandwidth Management			General, Bandwidth Policy, IPSec PassThrough Servers, Info
VPN Gateways			General, SSL, Traffic Trace, IP Pool, Host IP Address Pool, Host IP Pool, IP Sec, L2TP, NAP, Portal, Link Sets, Authorization, Groups, Authentication, Avaya Endpoint Access Control Agent, VPN Client, Accounting, SPO, and Advanced settings.
Administration			
	Operation	Host(s), Export/ Import Config, Software Upgrade, Language	Export/Import Cluster Configuration, Installed Packages, Upload New Package, Language List, Import/ Export Language Definition, Delete Language Definition.
	System	Time, NTP, DNS, Syslog, Trace, Static Routes	Add, Delete Save, Update
	Users	Passphrase, Password Expire Time	Add, Edit, Delete
	Remote Access	Telnet/SSH, Web	HTTP Settings, HTTP/SSL Settings, Idle Timeout
	Access List	Access List	Add
	SSH Keys	SSH Keys Generation	Add Import, Generate New Keys, Show SSH keys
	SNMP	General, SNMP Users, DISMAN Event MIB, System, Community, Notification Target, MIBs	Update, Add Event, Add Monitor, Save Download
	IP Pool	IP Pool List	Status
	SONMP	SONMP Settings	Status
	RADIUS	RADIUS Servers, Group Attributes	Add RADIUS Servers, Update

	RSA Server	RSA Server Add/ Update Page, Import sdconf.rec file	Update, Import
	Auditing	RADIUS Servers	Add
	In-Memory	General	Log status, update, Buffer Size
Dashboard			
	Health	Hosts, Alarms, Statistics	MIP and Host device details Alarms graph and details Statistics of servers
	Management	General Configuration, Logs, Users	Device status of Telnet, SSH, SONMP, Auditing, HTTP, HTTPS, SNMP, and RADIUS Logs graph and details Admin and CLI users, and resource usage graph
Monitor			

	Hosts	Management IP Address, Hosts Status	IP Address, MAC Address, Status Type, MIP, Local CPU Usage Memory Usage
	Disk Space Usage	Disk Space Usage	IP Address, MAC Address, Status, Type, MIP, Local, CPU %, Memory %
	Ethernet	Host Information, Receptions, Transmissions	Packets, Errors, Dropped, Overruns Frame
	Alarms	Alarm Table	Delete, Name, Sender, Cause, Severity, Time
	Users	Current Users	VPN, User, Login, Source IP, Host IP, Access, Group: Profile, Number Of Currently Logged In Users, Kick Selected, Kick All.
	SONMP Topology Table	SONMP Topology Table	Slot/Port, IP Address, Seg Id, MAC Address, Chassis Type, Local Seg, state.
	License Usage	Description	-
	IPsec Users	Description, IPsec Users	Number of Active IPsec Sessions, VPN, User, TunnelProfile, IP Inner/Outer, Encrypted, Decrypted Time

	Idle Users	Description	VPN, User, Login, Source IP, Active, Access
	BO Tunnel Sessions	Description, BO Tunnel Sessions	Number of Enabled BO Tunnel Sessions, Number of BO Tunnel Sessions in State VPN, BO Tunnel Profile, Host, State, Encrypted, Decrypted, Time
	IP Pool Allocations		IP Pool Allocations for all VPNs
	GUI Lock	GUI and VPN Locks	User Name, Lock Time, User Message, Take The Lock, Release The Lock
	CLI Logins	CLI Login Sessions	Logged In On, From, Kill Sessions
	About	Product Information	Product, version
Statistics			
	Authentication	Cluster Wide Authentication Statistics.	Servers, Accepted, Rejected, VPN, Timed Out
	SSL server	General, License, Cluster statistics, Cluster Histograms, Host statistics, Host Histograms	Active Request Sessions, Total Completed Request Sessions, Total Completed SSL Accept, Total Completed SSL Connect.
	IP Sec		
		General	IPsec Server Statistics, Clear all IPsec Statistics for all IPs
		Cluster	Cluster wide IPsec Statistics for VPN #
		Host	Single Host IPsec Statistics for VPN #
		BO Tunnels	General, Cluster statistics, Cluster Histograms, Host statistics, Host Histograms
	Bandwidth Management		Host Number, BWM Type, Refresh
Diagnostics			

	Events	Description, Events, Time frame, Events for	Host, Begin, End
	Audit Log	Description, Auditing, Time Frame, Audit Log	Host, Begin, End for
	Maintenance	Check configuration, Trace, In memory Log, Tech support dump	Stop Trace, Start Trace, Check Applied Configuration, Applied Configuration, Start logging, Stop logging, Clear logging, Maintenance Dump, Dump Log, Dump Statistics.

CHAPTER 4
VPN Introduction

This chapter introduces the VPN (Virtual Private Network) subsystem included in the Avaya VPN Gateway software.

The VPN subsystem is added on to the SSL acceleration subsystem, which makes it possible to combine SSL acceleration and VPN.

For more information about SSL acceleration, see the *Application Guide for SSL Acceleration*.

Secure Access from a Remote Location

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 is 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.

The intranet's resources can be accessed in clientless mode, transparent mode or both:

- ***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 page 67).
- ***Transparent mode***. From a computer with the Net Direct or the Avaya VPN Client in IPSec mode installed. The term "transparent" means that the remote user will experience network access as if actually sitting within the corporate intranet (see page 70).

VPNs

Up to 250 VPNs can be configured for each cluster of Avaya VPN Gateways. A VPN is typically defined for access to an intranet, parts of an intranet or to an extranet. For each VPN you can define the authentication methods to be used, which user access groups are authorized to the domain and the access rules that apply to each user group.

Each VPN has one or more IP addresses to which the remote user should connect to access resources on the intranet.

Secure Service Partitioning

Because the Avaya VPN Gateway software provides the ability to partition a cluster of Avaya VPN Gateways into separate VPNs, Internet Service Providers (ISPs) are provided with an excellent basis for hosting multiple VPN customers on a shared Remote Access Services (RAS) platform.

To enable the Secure Service Partitioning feature, a license key must be obtained from Avaya. For more information about the Secure Service Partitioning feature, see Chapter 17, “Secure Service Partitioning”.

Clientless Mode

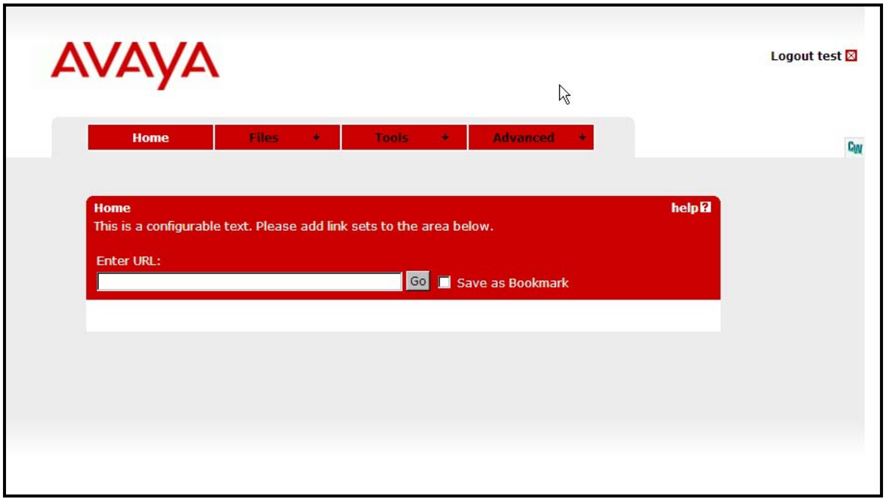
For a partner or mobile worker to access intranet resources from any computer with Internet connectivity (an Internet café or similar), access is made possible through the clientless mode. No manual software installation is required.

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 Avaya 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. Each VPN is provided with a web Portal where the remote user can access intranet resources from different tabs.



Home

This is a configurable text. Please add link sets to the area below.

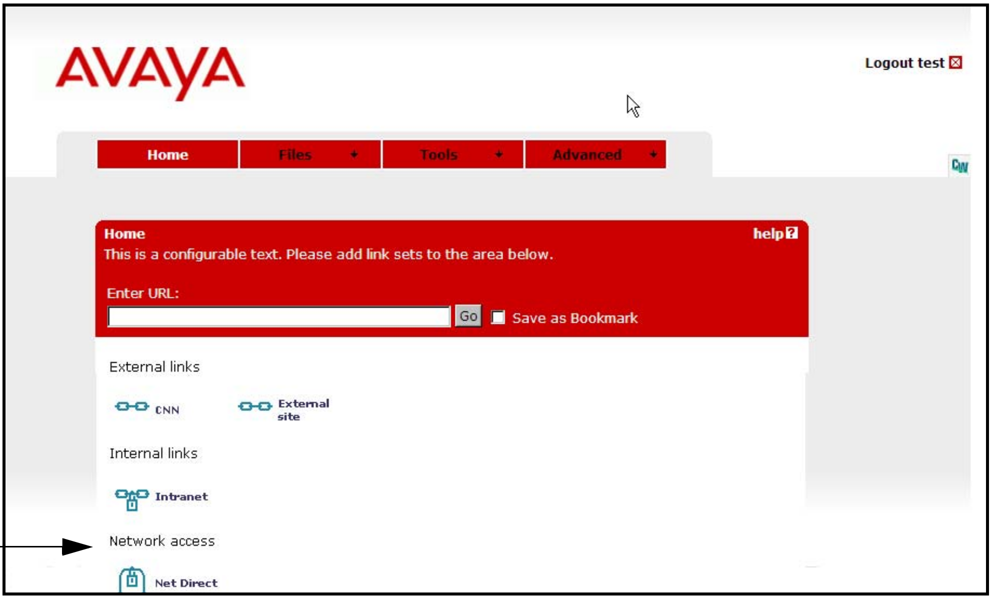
Enter URL:

□ Save as Bookmark

For a more detailed description of the Portal, see Chapter 6, "The Portal from an End-User Perspective".

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.



This is a configurable text. Please add link sets to the area below.

Net Direct link

Cached Version

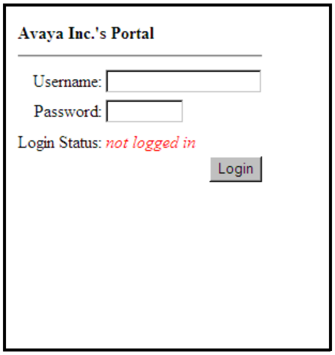
To cut down on network traffic and start-up time, a cached version of Net Direct is also available as a configurable option. If enabled, Net Direct leaves some components from the first installation on the client machine when the user exits the Portal session. These components can only be retrieved from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

Installed Version

The Net Direct client is also available as a setup.exe file to be installed permanently on the remote users' machines. See page 70.

PDA Support

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



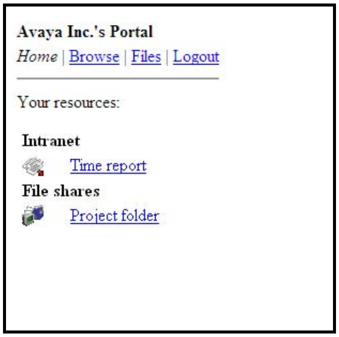
Avaya Inc.'s Portal

Username:

Password:

Login Status: *not logged in*

Once logged in, the PDA Portal is displayed. 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). The company name can be changed if desired.



Avaya Inc.'s Portal

Home | Browse | Files | Logout

Your resources:

Intranet

Time report

File shares

Project folder

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.

For instructions on how to configure the Avaya VPN Gateway for clientless mode, see Chapter 5, “Clientless Mode”.

Transparent Mode

As opposed to clientless mode, transparent mode requires the user to install VPN client software, either the Net Direct or the Avaya VPN Client. The Avaya 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.

Avaya 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 Avaya VPN Gateway cluster.

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

For more information about the Avaya VPN Client along with configuration instructions, see Chapter 21, “Transparent Mode”.

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 Chapter 7, “Net Direct”.

VPN Client Summary

As mentioned previously in this chapter, the Avaya VPN Gateway 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, Vista, 7	No
Net Direct (installable client)	SSL	All IP protocols	Windows 2000, XP, Vista, 7	Yes
Avaya VPN Client 10.06	SSL and IPsec	All IP protocols	Windows XP, Vista, Win 7 (32 and 64 bit)	Yes

Authentication and Access Control

To achieve secure authentication and access control, the Avaya VPN Gateway can use both external authentication servers and the Avaya 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.

External Database Authentication

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

Local Database Authentication

If no external authentication server exists, or if speedy deployment is required, the Avaya 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 Avaya VPN Gateway. 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 Chapter 8, "Groups, Access Rules and Profiles" you will find instructions on how to define groups, access rules and profiles.

Licenses

The following licenses are available to enhance the capabilities of the Avaya VPN Gateway software:

SSL License

To enable the VPN feature for more than 50 concurrent SSL users, a license key must be obtained from Avaya. SSL users are users connecting to the Avaya VPN Gateway through their web browsers or through the Avaya VPN Client. License upgrades are available for 50, 100, 250, 500, 1000 and 2000 users.

IPsec License

To enable the VPN feature for more than 50 concurrent IPsec users, a license key must be obtained from Avaya. IPsec users are users connecting to the Avaya VPN Gateway through the Avaya VPN Client. License upgrades are available for 250, 500, and 1000 users. For the ASA 310 and ASA 410 models, only demo licenses are available.

Secure Service Partitioning License

To enable the Secure Service Partitioning license, a license key must be obtained from Avaya. For more information about the Secure Service Partitioning feature, see Chapter 17, “Secure Service Partitioning”.

Portal Guard License

To enable the Portal Guard feature, a license key must be obtained from Avaya. For more information about the Portal Guard feature, see Chapter 22, “Configure Portal Guard”.

TPS License

A TPS (transactions per second) license is available for all other hardware models. No license is required to enable full TPS capacity.

Demo License

To try out the preceding features, a 30-day demo license can be obtained from Avaya upon request.

Virtual Desktop

To enable the virtual desktop feature, a license key must be obtained from Avaya. See Appendix A, “Virtual Desktop” for more information.

Emergency Remote Access License

An Emergency Remote Access (ERA) license provides remote access in a secure way. The ERA license is valid for 60 days. License upgrades are available for 500, 1000, 2000, and 5000 users.

NOTE – The license validity period can be extended by contacting Avaya support.

Secure Portable Office License

To enable the Secure Portable Office feature, a license key must be obtained from Avaya. See Chapter 13, “Secure Portable Office Client” for more information.

Obtaining Licenses

This section details the procedure necessary for obtaining license and applying it to the device.

To obtain the licenses, perform this procedure.

1. **Contact Avaya to purchase an Application Acceleration License.**

   To obtain an Avaya license ensure you have the correct product code and go to www.avaya-datalicensing.com.

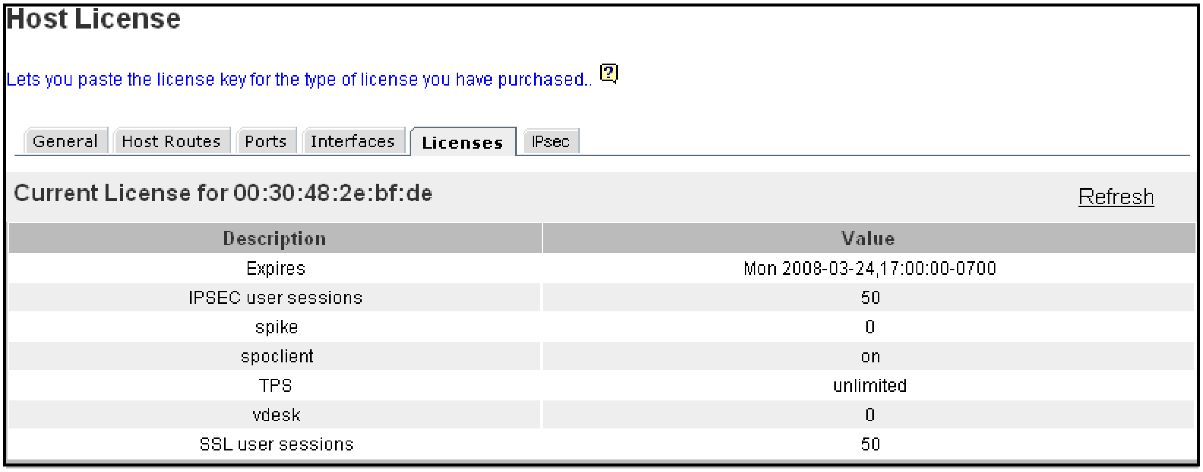
   To contact Avaya, see www.avaya.com/support

   The device MAC address can be obtained by using the /info/local command in the CLI.

   ```
   >> Main# /info/local
   ```

   To acquire the cluster master MAC address, use this command in conjunction with the Cluster Management IP Address. To acquire a slave’s MAC address, use this command while logged into the CLI of the individual slave.

NOTE – You can view the MAC address by selecting **Host** > **License.** In the following screen, **00:30:48:2e:bf:de** is the MAC address.



Host License

Lets you paste the license key for the type of license you have purchased..

Current License for 00:30:48:2e:bf:de

Description	Value
Expires	Mon 2008-03-24,17:00:00-0700
IPSEC user sessions	50
spike	0
spoclient	on
TPS	unlimited
vdesk	0
SSL user sessions	50

2. **After the device MAC address is verified by Avaya, a keycode is sent to you. Use this keycode to enable the feature.**

   To apply the keycode to the device through the BBI, perform the following procedure.

3. **Select the Config tab.**

4. **Select Host > License from the BBI menu.**

5. **Paste the keycode in the text box labeled New License.**

6. **Click Save.**

NOTE – The keycode can be applied to the device through CLI. For information on this, see CLI Application Guide.

License Key

To obtain the license key from Avaya, you have to provide the MAC address of each Avaya VPN Gateway device on which a VPN license should be installed (see instructions on next page). This applies to all available licenses.

License Pool (SSL and IPsec Users)

All Avaya VPN Gateways that are up and running in a cluster contribute to the license pool. For example, if the cluster consists of two Avaya VPN Gateways – where each device has an IPsec license installed that is valid for 500 users – the cluster shares a license pool of 1000 concurrent IPsec users. When the remote user connects to the Avaya VPN Gateway cluster, a license for the current user session is allocated from the license pool – not from a specific Avaya VPN Gateway. The distribution of users on the two devices is independent of the licenses installed on each device.

If a user logs in through IPsec and there is no IPsec user license available, an SSL user license will instead be used (if available).

If a Cluster Member Fails

If a cluster member fails, it will continue to contribute to the license pool for a period of 30 days. After that, the cluster will no longer be aware of the license loaded to the faulty device. Using the preceding example, the license pool would only consist of a 500 user license after the 30 day grace period.

If the cluster consists of three Avaya VPN Gateways – one with a 1000 user license and the two other devices with the default 50 user license – the license pool will only consist of a 100 user license (after 30 days) if the Avaya VPN Gateway with the 1000 user license fails.

An alarm message is generated if the devices in a cluster do not have the same license loaded. In the SSL/IPsec user license case, this message can safely be ignored. In the Secure Service Partitioning case however, the licenses must be the same on all devices.

Also see the section “If a Cluster Member Fails” on page 81.

Secure Portable Office

The Secure Portable Office feature does not work properly in a cluster unless this feature is enabled by license key on every device in the cluster.

Secure Service Partitioning

The Secure Service Partitioning feature will not work properly on all devices unless this feature is unlocked on *every* Avaya VPN Gateway in the cluster, using a unique Secure Service Partitioning license key.

Hardware Limits

Loaded licenses in a cluster might add up to a high total number of allowed users. Each device type however has a hardware limit that determines how many concurrent user sessions it can accept.

- Avaya VPN Gateway 3090-VM: 5000 SSL concurrent users. The single node host license limit is 5000.

NOTE – The 3090-VM requires the Enterprise VMware license or VMware ESX 4.1 and above license to enable 8-core in Guest OS environment.

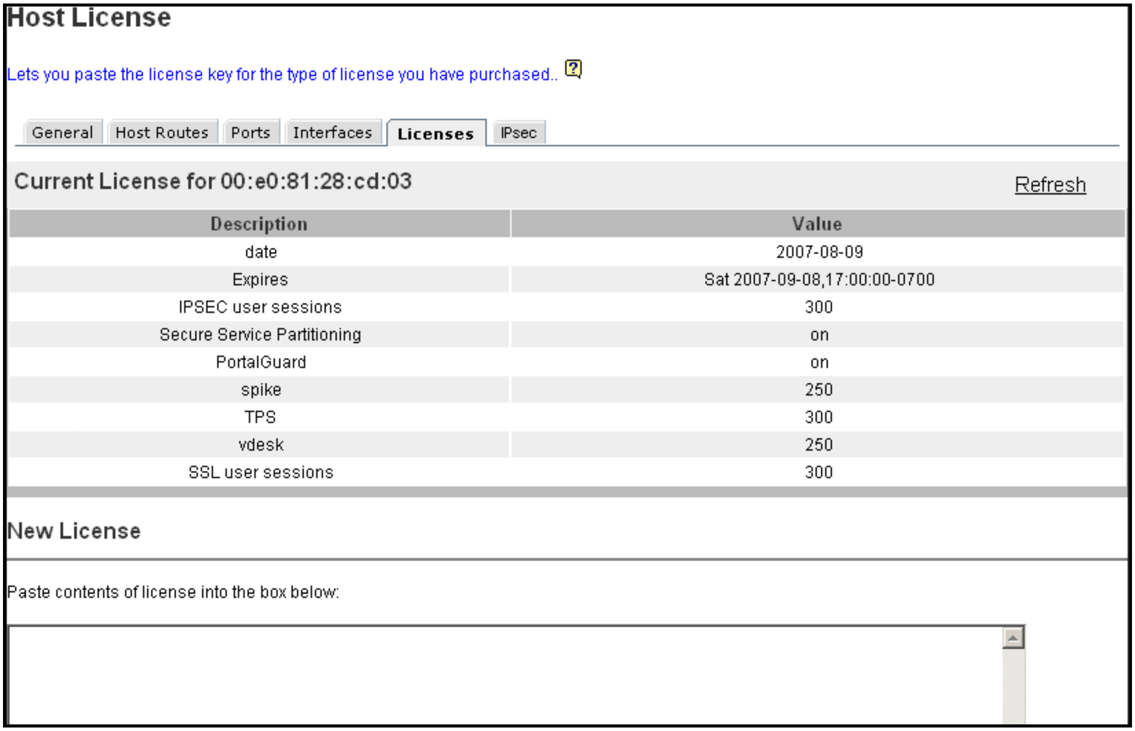
- Avaya VPN Gateway 3070-VM: 1000 concurrent users
- Avaya VPN Gateway 3050-VM: 250 concurrent users

For example, if the cluster consists of two Avaya VPN Gateways, each with a 5000 user license, make sure that the cluster is properly load balanced to avoid an uneven session distribution.

How to Obtain the MAC Address

1. **Log in to the BBI as administrator user.**
2. **Click on config tab and select Host(s).**
3. **Double click on the host name.**
4. **Click on Licenses tab.**

   The Host License form is displayed.



Host License

Lets you paste the license key for the type of license you have purchased..

Current License for 00:e0:81:28:cd:03

Description	Value
date	2007-08-09
Expires	Sat 2007-09-08,17:00:00-0700
IPSEC user sessions	300
Secure Service Partitioning	on
PortalGuard	on
spike	250
TPS	300
vdesk	250
SSL user sessions	300

New License

Paste contents of license into the box below:

5. **Contact Avaya Support and provide the MAC address. You will be given the license key for the desired number of users.**

Paste the License Key

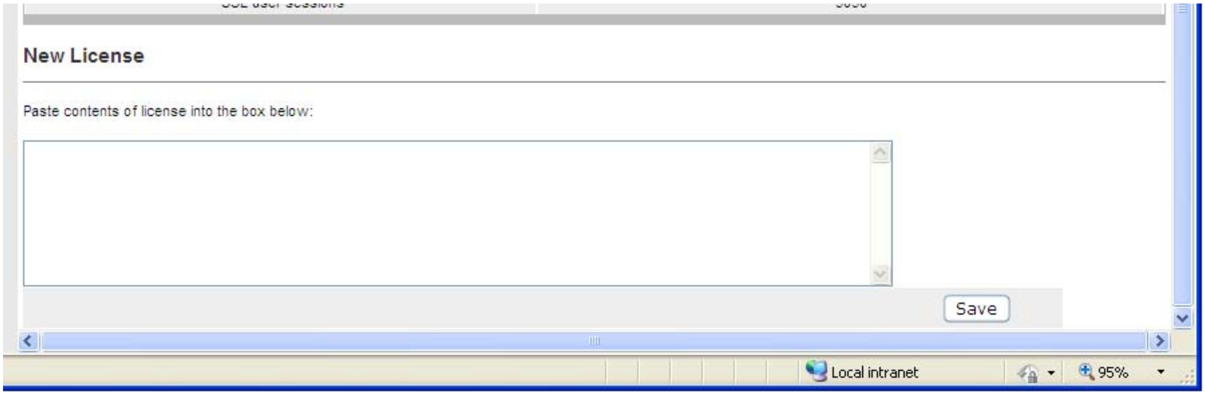
1. **Log in to the BBI as administrator user.**

2. **Click on config tab and select Host(s).**

3. **Double click on the hostname.**

   The Host License form is displayed.

4. **Scroll down to New License.**



New License

Paste contents of license into the box below:

5. **Paste the license key into the box. Include the BEGIN LICENSE and END LICENSE lines.**

6. **Click Save.**

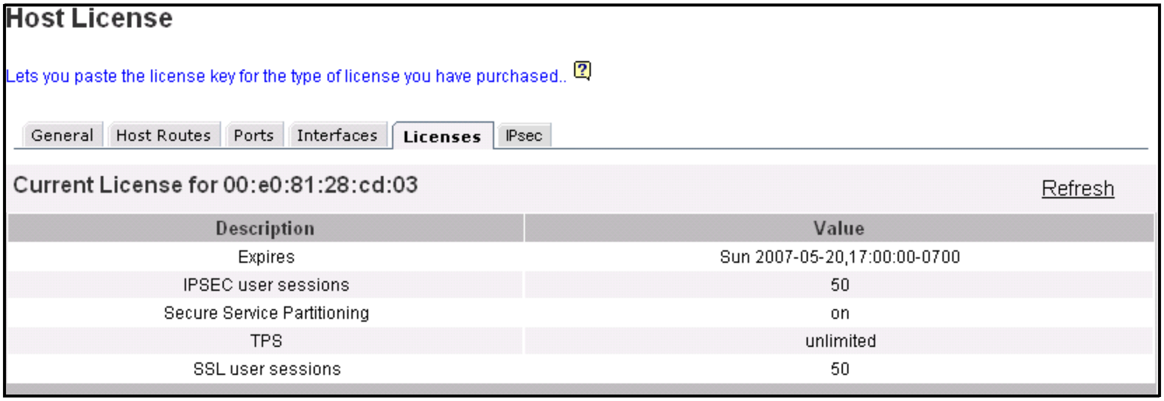
7. **To load a license key to another Avaya VPN Gateway in the cluster, select the desired device in the Host field, then paste the license into the box.**

   Note that this must be another license key, because each key is generated from the Avaya VPN Gateway's MAC address.

NOTE – If there are several Avaya VPN Gateways in the cluster and they do not have the same license loaded, a warning message is generated.

If there are active alarms, the administrator is notified on login. The alarm can be viewed in the Alarm list (Administration>Monitor>Alarms) and the System log (Diagnostics>Events).

This is what the License form will look like with a multi-license key loaded. The form includes information about the license key's expiration date.



Host License

Lets you paste the license key for the type of license you have purchased..

Current License for 00:e0:81:28:cd:03

Description	Value
Expires	Sun 2007-05-20,17:00:00-0700
IPSEC user sessions	50
Secure Service Partitioning	on
TPS	unlimited
SSL user sessions	50

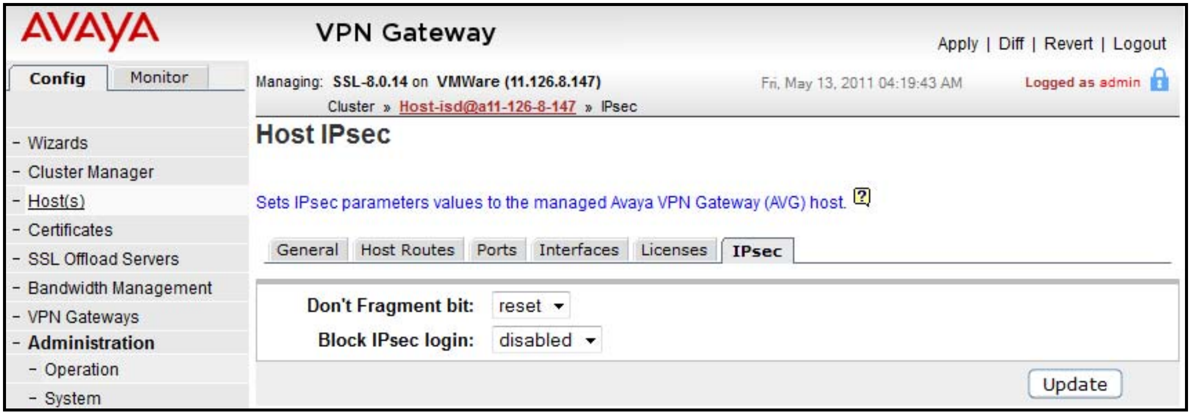
Manage new IPsec logins during maintenance

The option “Disable new IPSec logins” allows maintenance of the VPN Gateway without forcing current users to log-off. During the maintenance interval, new IPSec logins to the node can be redirected to the other nodes.

1. **Click the Config tab in the navigation pane.**
2. **Click the Host(s) tab in the navigation tree.**
3. **Double-click on the host under maintenance.**

   The System Information window appears.
4. **Click the IPsec tab in the System Information window.**

   The Host IPsec pane appears.



Managing: SSL-8.0.14 on VMWare (11.126.8.147)   Fri, May 13, 2011 04:19:43 AM   Logged as admin

Cluster » Host-isd@a11-126-8-147 » IPsec

Host IPsec

Sets IPsec parameters values to the managed Avaya VPN Gateway (AVG) host.

Don't Fragment bit: reset

Block IPsec login: disabled

5. **Select the fragment bit option in the Don't Fragment Bit pull-down menu.**

   The default value is copy.

6. **Select the block login option from the Block IPsec Login field.**

   The default is disabled.

7. **Click the Update button to save the change.**

If a Cluster Member Fails

If a cluster member fails it will continue to contribute to the license pool for a period of 30 days. When the 30 days have expired, the cluster will no longer be aware of the license loaded to the faulty device. If the device must be replaced, proceed as follows (the instruction refers to the CLI management interface):

1. **Contact your reseller at Avaya for information about the possibilities of a replacement device and license.**

   When you have obtained a new device and a new license, continue with the following steps.

2. **Dump the information configured for the faulty device (host).**

```
>> Main# cfg/sys/host 2/dump
Dump private/secret keys (yes/no) [yes]: <press ENTER to accept>
Collecting data, please wait...
```

3. **Copy and save the data to a text editor.**

4. **Delete the faulty host from the cluster.**

```
>> Main# cfg/sys/host 2/delete
Cluster Host 2 will be deleted when changes are applied.
```

5. **Connect the new device to the network and join it to the cluster.**

   For instructions on how to join an Avaya VPN Gateway to an existing cluster, see the “Initial Setup” chapter in the *User’s Guide*. Assign the IP address of the failed device to the new device.

6. **Load the license to the new device as described in the section "Paste the License Key" on page 78.**

   Note that a new license is needed because the new device has a different MAC address.

7. **To restore the host configuration, paste the configuration that was previously dumped.**

```
>> Main# cfg/sys/host 2/paste
Enter global key/secret import password: <press ENTER to skip>
>> Cluster Host 1#  <paste the configuration at this prompt>
```

8. **Apply the changes.**

CHAPTER 5

Clientless Mode

This chapter describes how to configure the Avaya VPN Gateway for clientless mode. Clientless mode does not require any reconfiguration of the client web browser, nor does any VPN client software need to be installed on the remote user's machine.

Following is a simple overview of the flow when a remote user requests a resource on the intranet. To access the Portal, the remote user types the Avaya VPN Gateway's Portal IP address or fully qualified domain name in the available browser. The Portal's capabilities are shown in the Intranet cloud in the illustration. To maintain the Avaya VPN Gateway configuration (for example add users, change access rules and so on), the operator connects to the Avaya VPN Gateway's management IP address (MIP). To access the command line interface (CLI), the operator connects to the MIP through Telnet or SSH. To access the browser-based management interface (BBI), the operator connects to the MIP through the browser.

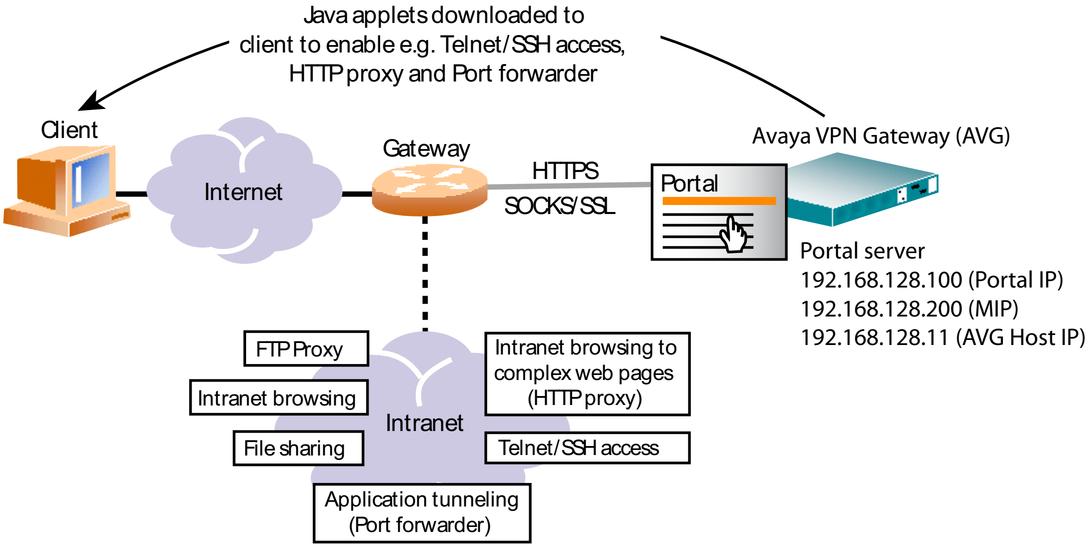


Figure 5-1 VPN in Clientless Mode

Configure VPN from Wizard Settings

If you run the VPN Quick Setup wizard during the initial setup procedure, the Avaya VPN Gateway cluster is automatically configured with all the required settings for a fully functional VPN Portal (clientless mode), as well as support for the Avaya VPN Client (transparent mode). This setup is mainly for testing purposes but you can easily let your proper VPN evolve from these settings.

The following settings have been created:

- A VPN with the number 1.
- A server of the portal type with a Portal IP address. This is the address to which the remote user should connect to access the Portal. The portal server is set to standalone mode, which is required when using the VPN feature without an application switch.
- A test certificate has been installed for use with the portal server.
- You have had the option to add one or several domains to the DNS search list, which means that the remote user can enter a short name in the Portal's various URL and host name fields (for example `inside` instead of `inside.example.com` if `example.com` is added to the search list).
- The authentication method is set to Local database and you have one test user configured, belonging to a group called `trusted`. The `trusted` group's access rules allow access to all networks, services and paths.

Having tested the Portal, the next step is to make all the necessary adjustments to the settings made by the wizard. You probably want more than one user and one access group configured and the relevant access rules have to be defined for each group. The test certificate should be substituted for a real certificate, signed by a CA authority. Furthermore, you may want to use an external authentication database instead of or, as a complement, to the local database.

The following sections describe how to import a signed server certificate, map it to the VPN and how to configure a DNS name.

For information about how to perform an initial setup, see the "Initial Setup" chapter in the *User's Guide*.

Create a Test Certificate

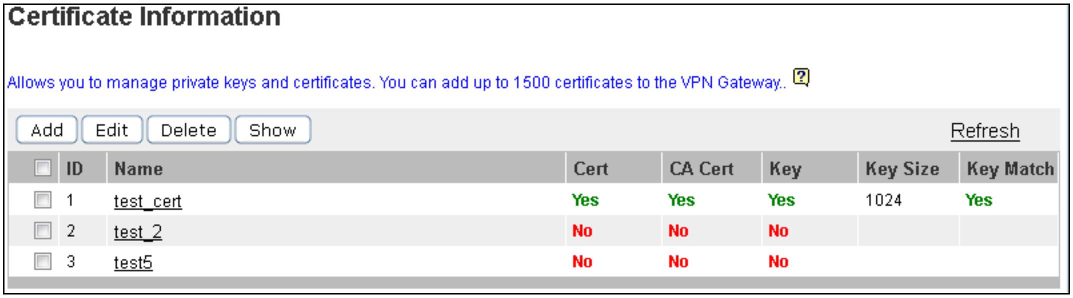
Follow these steps to create a Test Certificate:

1. **Log in to the BBI as administrator.**

2. **Click on Config tab.**

3. **In the system tree view, select Certificates.**

   The test certificate is created when you run the VPN Quick setup wizard. If you have not run the VPN Quick setup wizard, no certificates are displayed.

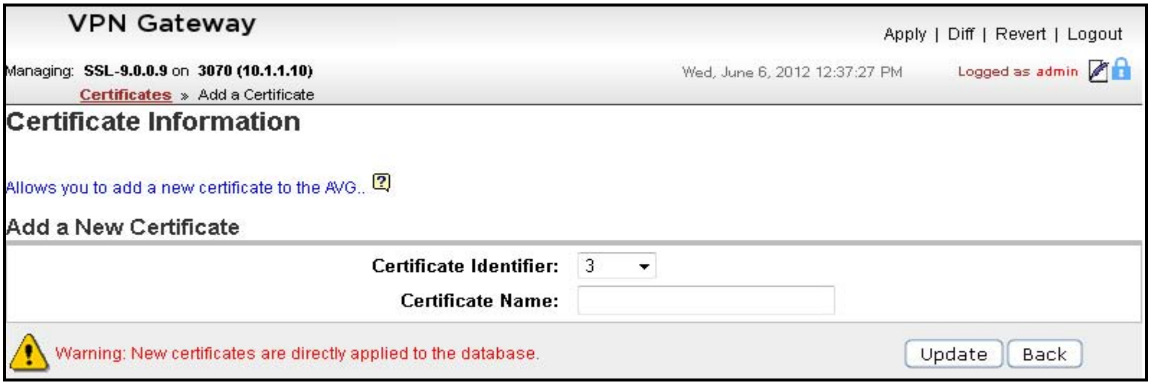


Certificate Information

Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		

4. **Click Add.**



VPN Gateway

Managing: SSL-9.0.0.9 on 3070 (10.1.1.10)   Wed, June 6, 2012 12:37:27 PM   Logged as admin

Certificates » Add a Certificate

Certificate Information

Allows you to add a new certificate to the AVG..

Add a New Certificate

Certificate Identifier:	3
Certificate Name:	

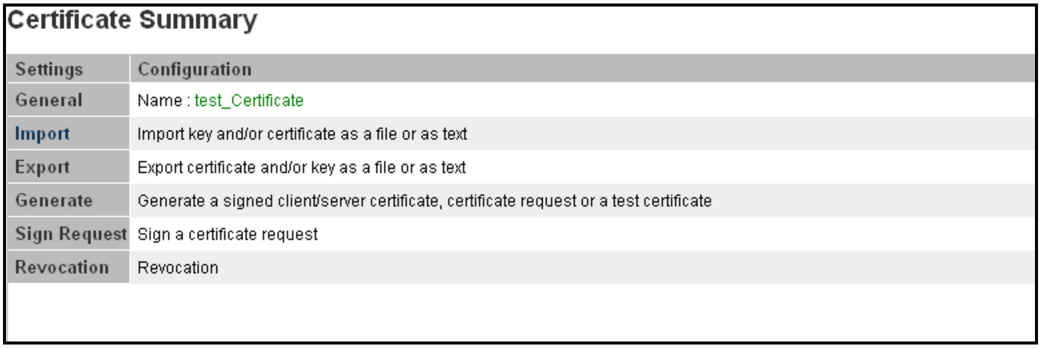
Warning: New certificates are directly applied to the database.

5. **Click Update.**

   A place holder for the new certificate is created.

6. **Click on the name of the certificate.**

Certificate summary screen is displayed.



Certificate Summary

Settings	Configuration
General	Name : test_Certificate
Import	Import key and/or certificate as a file or as text
Export	Export certificate and/or key as a file or as text
Generate	Generate a signed client/server certificate, certificate request or a test certificate
Sign Request	Sign a certificate request
Revocation	Revocation

7. **Under settings, click Generate.**

   By default Generate Signing Request screen is displayed.

8. **Click Test Certificate tab.**

9. **Specify name of the Web server in the Common Name field as it appears in the URL.**

   This name must be the same as the domain name of the Web server that is requesting a certificate. Wildcards (such as * or ?) and IP address are not allowed.

10. **Click Update.**

11. **Click Apply to save.**

Import Signed Certificate to the Avaya VPN Gateway

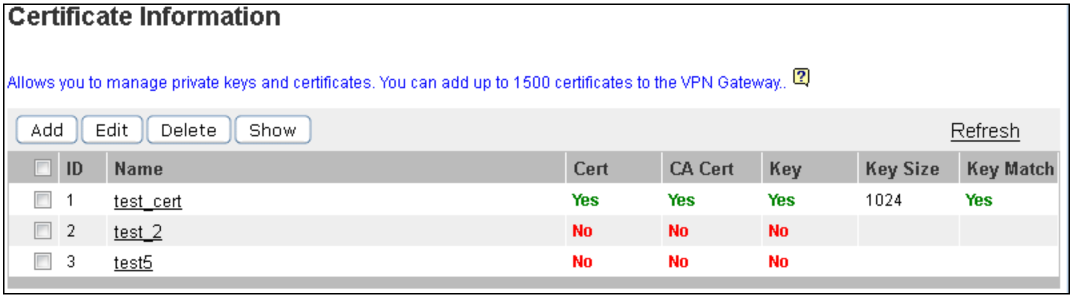
This instruction assumes that you have a real server certificate available, signed by a CA authority. The certificate can be imported to the Avaya VPN Gateway as a file, through the BBI, or be pasted into the BBI as text.

1. **Log in to the BBI as administrator.**

2. **Click on Config tab.**

3. **In the system tree view, select Certificates.**

The test certificate is created when you run the VPN Quick setup wizard. If you have not run the VPN Quick setup wizard, no certificates are displayed.

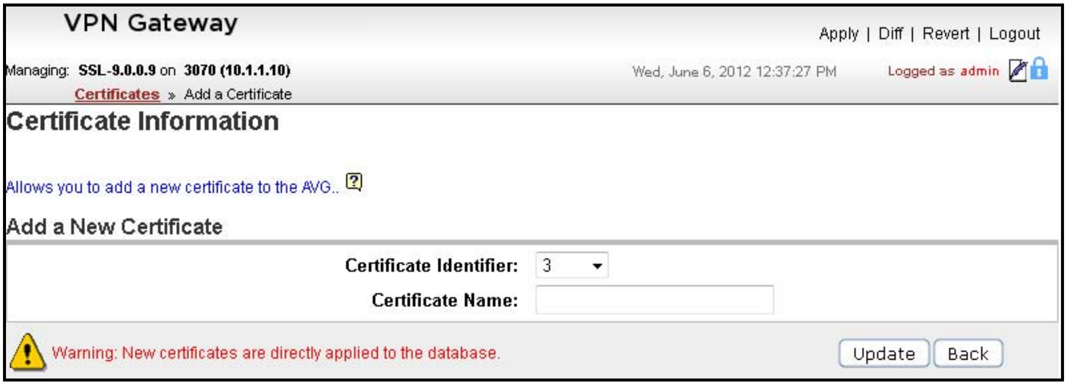


Certificate Information

Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		

4. **Click Add.**



VPN Gateway

Managing: SSL-9.0.0.9 on 3070 (10.1.1.10)   Wed, June 6, 2012 12:37:27 PM   Logged as admin

Certificates » Add a Certificate

Certificate Information

Allows you to add a new certificate to the AVG..

Add a New Certificate

Certificate Identifier:	3
Certificate Name:	

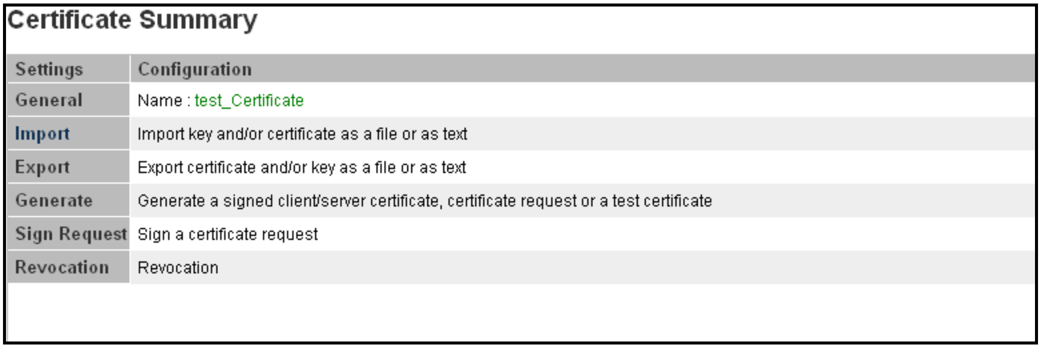
Warning: New certificates are directly applied to the database.

5. **Click Update.**

   A place holder for the new certificate is created.

6. **Click on the name of the certificate.**

Certificate summary screen is displayed.

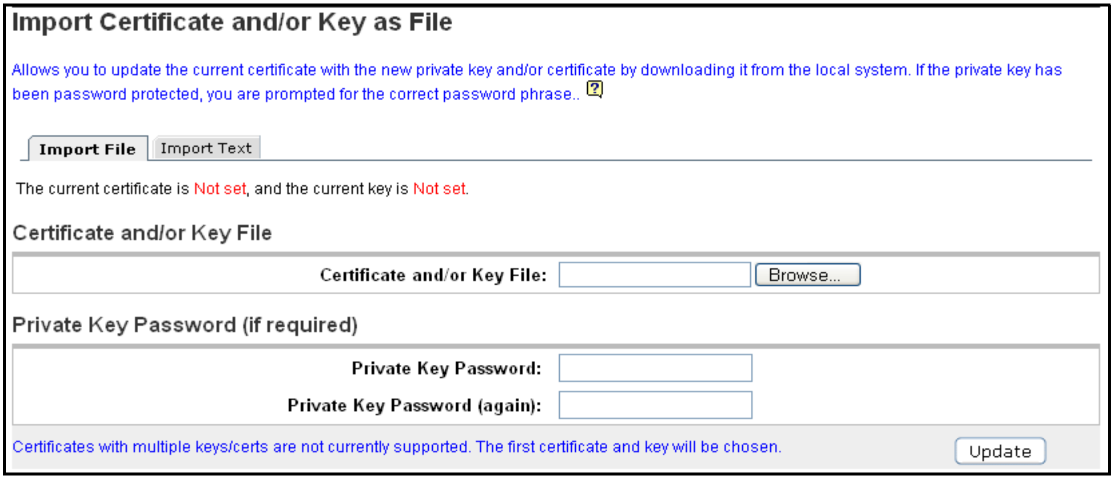


Certificate Summary

Settings	Configuration
General	Name : test_Certificate
Import	Import key and/or certificate as a file or as text
Export	Export certificate and/or key as a file or as text
Generate	Generate a signed client/server certificate, certificate request or a test certificate
Sign Request	Sign a certificate request
Revocation	Revocation

7. **To import a file, click Import.**

   Import Certificate screen is displayed.



Import Certificate and/or Key as File

Allows you to update the current certificate with the new private key and/or certificate by downloading it from the local system. If the private key has been password protected, you are prompted for the correct password phrase..

The current certificate is Not set, and the current key is Not set.

Certificate and/or Key File

Certificate and/or Key File:

Private Key Password (if required)

Private Key Password:

Private Key Password (again):

Certificates with multiple keys/certs are not currently supported. The first certificate and key will be chosen.

8. **Under Certificate and/or Key file, click Browse.**

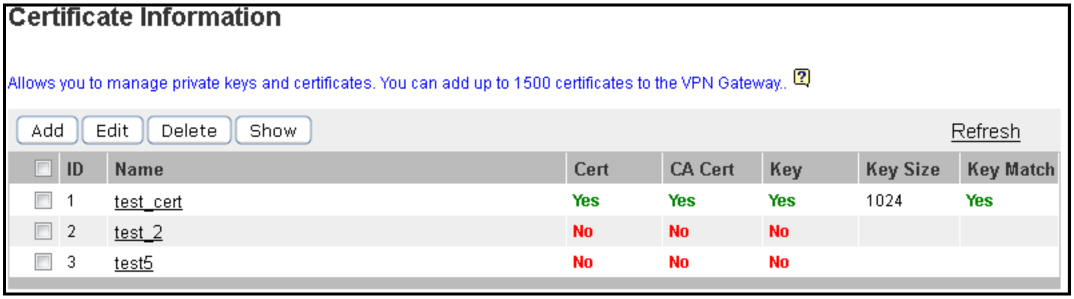
   The files in your file system are displayed.

9. **Find and double-click the certificate file you wish to import.**

10. **In the fields under Private Key Password, enter the import passphrase if required.**

11. **Click Update.**

12. **In the System tree view, select Certificates to view the properties of the imported certificate.**



Certificate Information

Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

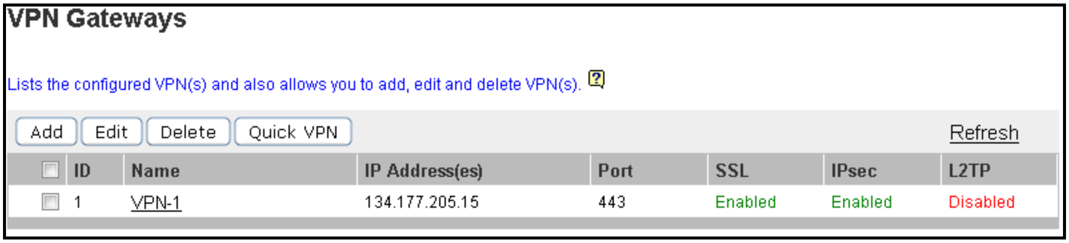
□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		

13. **Apply the changes.**

Map Signed Server Certificate to VPN

When the signed server certificate has been added to the Avaya VPN Gateway, it should be mapped to the portal server of the desired VPN. The certificate (with certificate no 1) that is currently mapped to your portal server is a self-signed test certificate. Select the number corresponding to the signed certificate that you have added to the Avaya VPN Gateway.

1. **Log in to the BBI as administrator.**
2. **Click on Config tab.**
3. **In the system tree view, select VPN Gateways.**



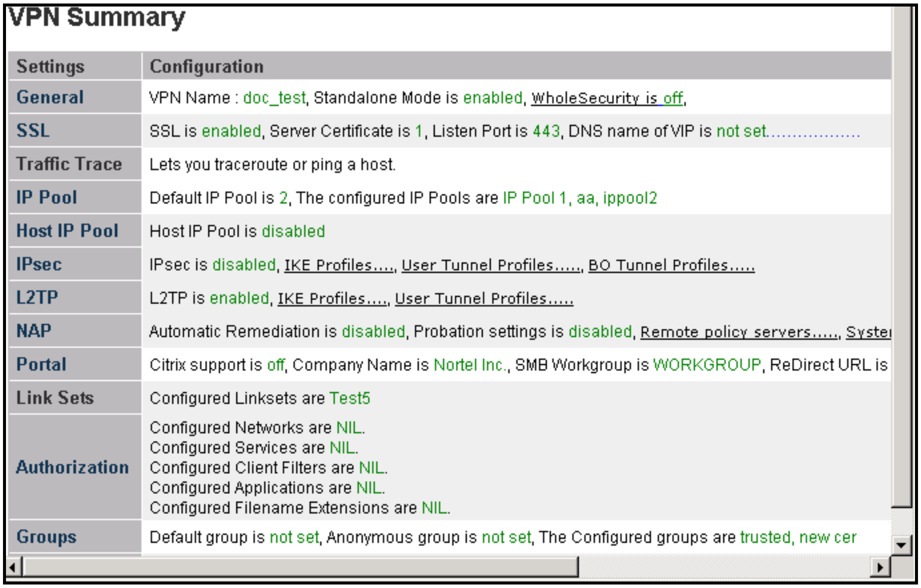
VPN Gateways

Lists the configured VPN(s) and also allows you to add, edit and delete VPN(s).

□	ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP
□	1	VPN-1	134.177.205.15	443	Enabled	Enabled	Disabled

4. **Click on VPN Gateway name.**

VPN Summary screen is displayed.

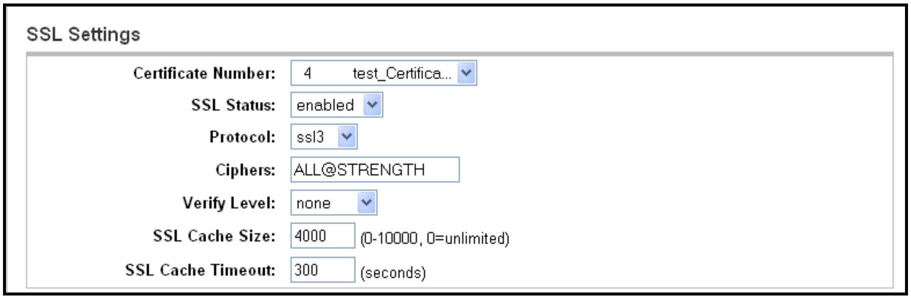


VPN Summary

Settings	Configuration
General	VPN Name : doc_test, Standalone Mode is enabled, WholeSecurity is off,
SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is not set.................
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 2, The configured IP Pools are IP Pool 1, aa, ippool2
Host IP Pool	Host IP Pool is disabled
IPsec	IPsec is disabled, IKE Profiles....., User Tunnel Profiles....., BO Tunnel Profiles.....
L2TP	L2TP is enabled, IKE Profiles....., User Tunnel Profiles.....
NAP	Automatic Remediation is disabled, Probation settings is disabled, Remote policy servers....., Syste
Portal	Citrix support is off, Company Name is Nortel Inc., SMB Workgroup is WORKGROUP, ReDirect URL is
Link Sets	Configured Linksets are Test5
Authorization	Configured Networks are NIL. Configured Services are NIL. Configured Client Filters are NIL. Configured Applications are NIL. Configured Filename Extensions are NIL.
Groups	Default group is not set, Anonymous group is not set, The Configured groups are trusted, new cer

5. **Click SSL.**

6. **Under SSL Settings, in the Certificate Number list box, select the certificate number you wish to map to the portal server.**



SSL Settings

Certificate Number:	4 test_Certifica...
SSL Status:	enabled
Protocol:	ssl3
Ciphers:	ALL@STRENGTH
Verify Level:	none
SSL Cache Size:	4000 (0-10000, 0=unlimited)
SSL Cache Timeout:	300 (seconds)

7. **Click Update.**

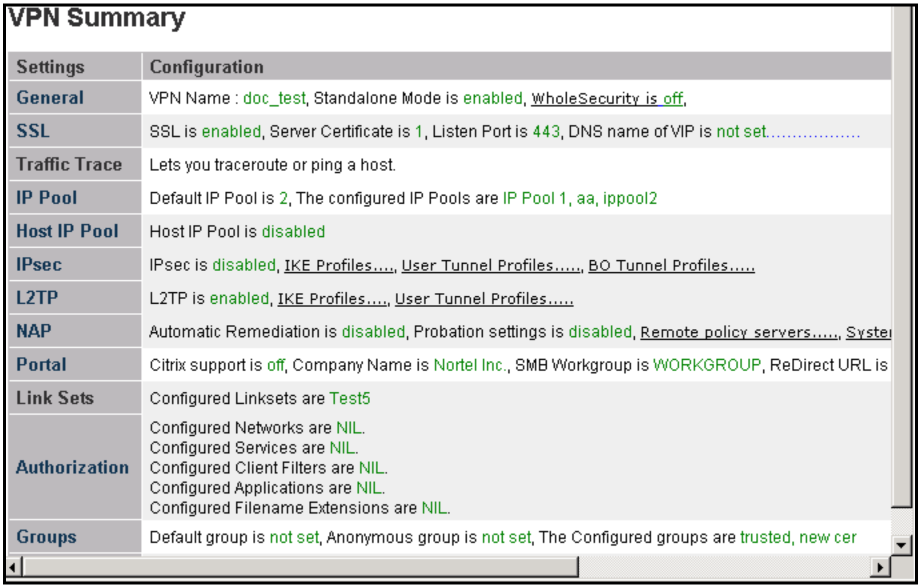
8. **Apply the changes.**

Assign a Fully Qualified Domain Name (FQDN)

This step assigns a FQDN to the portal server. The domain name you specify should be registered in DNS to resolve to the virtual server IP address you specified in VPN quick setup wizard. The FQDN for the portal server corresponds to the URL that remote users will type in the address field of their web browser to access the Portal login page.

1. **Log in to the BBI as administrator.**
2. **Click on Config tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Click on VPN Gateway name.**

   VPN Summary screen is displayed.



VPN Summary

Settings	Configuration
General	VPN Name : doc_test, Standalone Mode is enabled, WholeSecurity is off,
SSL	SSL is enabled, Server Certificate is 1, Listen Port is 443, DNS name of VIP is not set.................
Traffic Trace	Lets you traceroute or ping a host.
IP Pool	Default IP Pool is 2, The configured IP Pools are IP Pool 1, aa, ippool2
Host IP Pool	Host IP Pool is disabled
IPsec	IPsec is disabled, IKE Profiles...., User Tunnel Profiles....., BO Tunnel Profiles.....
L2TP	L2TP is enabled, IKE Profiles...., User Tunnel Profiles.....
NAP	Automatic Remediation is disabled, Probation settings is disabled, Remote policy servers....., Syste
Portal	Citrix support is off, Company Name is Nortel Inc., SMB Workgroup is WORKGROUP, ReDirect URL is
Link Sets	Configured Linksets are Test5
Authorization	Configured Networks are NIL. Configured Services are NIL. Configured Client Filters are NIL. Configured Applications are NIL. Configured Filename Extensions are NIL.
Groups	Default group is not set, Anonymous group is not set, The Configured groups are trusted, new cer

5. **Click SSL.**
6. **In the DNS Name of VIP field, enter the FQDN, e.g. vpn.example.com.**
7. **Click Update.**
8. **Apply the changes.**

Now you have created the basis for your Portal. What remains to be done is to update your DNS server, configure one or more authentication methods, add user groups with access rules, configure group links and customize the web Portal page. You may also want to configure Net Direct, the Avaya Endpoint Access Control Agent client security feature and HTTP to HTTPS redirection.

For a list of the remaining tasks and where to find the necessary documentation, see page 95.

Configure VPN from Scratch

If you did not run the VPN quick setup wizard during the initial setup, this section describes how to configure the VPN from scratch. Even if you did run the VPN quick setup wizard, reading through this section will give you an idea about which settings are required for a fully functional Portal.

Import Signed Certificate

For instructions on how to import a signed certificate to be used as the Avaya VPN Gateway's server certificate, see "Import Signed Certificate to the Avaya VPN Gateway" on page 86.

Create a VPN

These steps create a VPN. You can have several VPNs, where each VPN identifies a unique Portal. Thus, you can have several different Portals, for example, with different layout and links. A portal server is automatically created along with the VPN. The portal server is connected to the Portal IP address(es) and listens to TCP port 443 (https) by default.

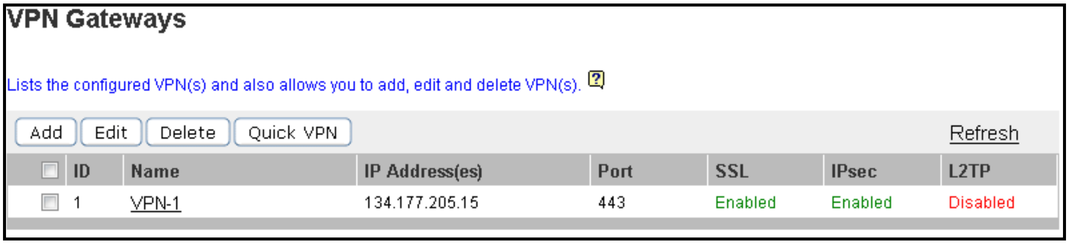
Creating several VPNs is especially useful for internet service providers (ISPs). It enables hosting of a number of customers with their own Portals, securely separated from one another (see Chapter 17, "Secure Service Partitioning").

1. **Log in to the BBI as administrator.**

2. **Click Config.**

3. **In system tree view, select the VPN Gateway name.**

The VPN Gateways form is displayed.



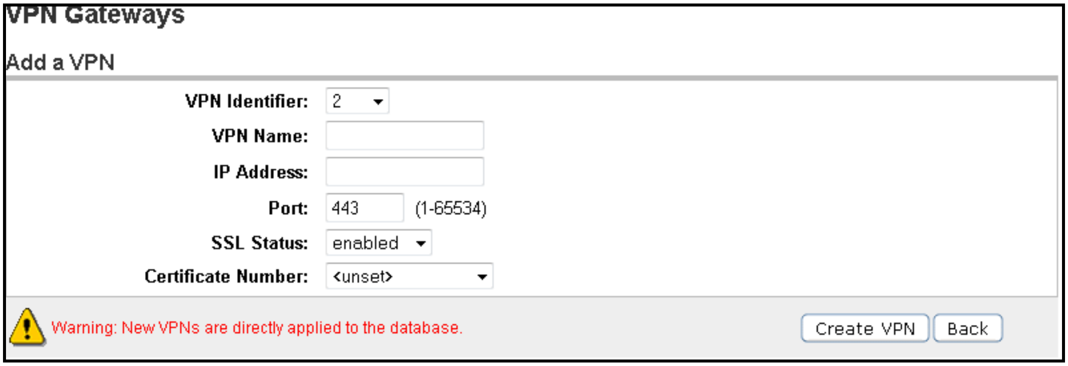
VPN Gateways

Lists the configured VPN(s) and also allows you to add, edit and delete VPN(s).

□	ID	Name	IP Address(es)	Port	SSL	IPsec	L2TP
□	1	VPN-1	134.177.205.15	443	Enabled	Enabled	Disabled

4. **Click Add.**

   The Add VPN form is displayed.



VPN Gateways

Add a VPN

VPN Identifier:	2
VPN Name:	
IP Address:	
Port:	443 (1-65534)
SSL Status:	enabled
Certificate Number:	<unset>

Warning: New VPNs are directly applied to the database.

5. **In the Name field (optional) enter a name for the VPN.**

6. **In the IP address field, enter the Portal IP address.**

   This is the IP address the remote user should use to connect to the VPN.

7. **In the Certificate Number list box, select the server certificate you wish to use.**

   This requires that you have previously imported a signed certificate to the Avaya VPN Gateway or that you have created a test certificate.

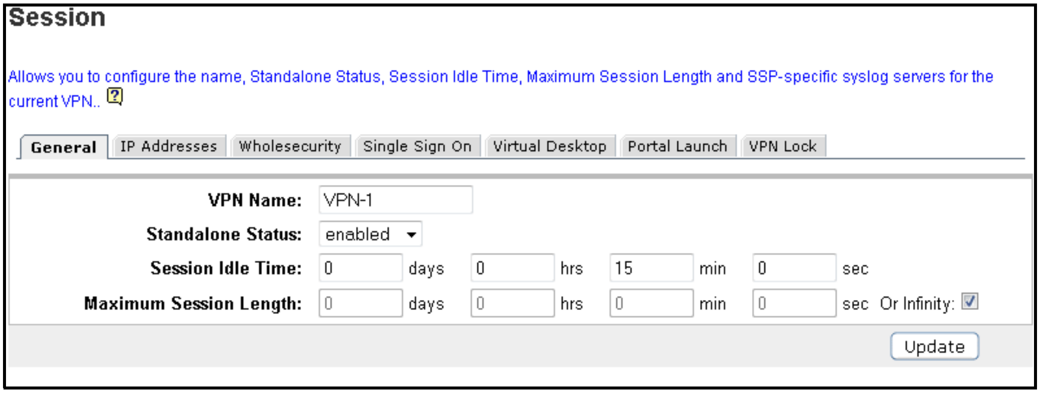
8. **Click Create VPN.**

   The new VPN is added to the VPN Gateways form.

9. **Click on the VPN Gateway name**

10. **Click on General settings.**

Session screen is displayed.



Session

Allows you to configure the name, Standalone Status, Session Idle Time, Maximum Session Length and SSP-specific syslog servers for the current VPN..

VPN Name: VPN-1

Standalone Status: enabled

Session Idle Time: 0 days 0 hrs 15 min 0 sec

Maximum Session Length: 0 days 0 hrs 0 min 0 sec Or Infinity: ☑

11. **Under General, set the standalone status.**

This step sets the portal server to standalone mode, which is required if the Avaya VPN Gateway is *not* connected to an application switch. Application switches can be used to load balance clusters of Avaya VPN Gateways to increase performance (see page 99).

12. **Click Update.**

13. **Click on SSL in VPN Summary screen.**

14. **In the DNS Name of VIP field, enter a Fully Qualified Domain Name (FQDN) for the portal server.**

The domain name you specify (for example vpn.example.com) should be registered in DNS to resolve to the virtual server IP address you specified in Step 6. The FQDN for the portal server corresponds to the URL that remote users will type in the address field of their web browser to access the Portal login page when the VPN is fully deployed.

15. **Expand VPN Gateways and Gateway Setup.**

16. **Select DNS.**

17. **Configure the desired search domains.**

The search domain(s) you specify are automatically appended to the host names a remote user types in the various address fields on the Portal (provided 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 only typing `inside` in the URL field displayed on the Portal’s Home tab.

If you specify more than one domain name, separate the names with comma (,).

18. **Click Update and apply your changes.**

Now you have created the basis for your Portal. What remains to be done is to update your DNS server, configure one or more authentication methods, add user groups with access rules, configure group links and customize the web Portal page. You may also want to configure Net Direct, the Avaya Endpoint Access Control Agent, Avaya Endpoint Access Control Agent client security feature and HTTP to HTTPS redirection.

To test the Portal, you can create a test group and configure the desired access rules for the group. Then enable the Avaya VPN Gateway's local user database, add a test user and map this user to the test group. See Chapter 8, "Groups, Access Rules and Profiles" and Chapter 9, "Authentication Methods", respectively.

Update DNS Server

The local DNS server should be updated with the domain name used for the VPN, and be configured to perform reverse DNS lookups.

Configure User Access Groups and Access Rules

The user's group membership determines what resources can be accessed from the Portal. The access rules associated with a group govern which networks, services and paths the group member should have access to. See Chapter 8, "Groups, Access Rules and Profiles" for configuration instructions.

Select Authentication Method(s)

Several different external authentication methods are available (RADIUS, LDAP, NTLM, CA SiteMinder, RSA ClearTrust and RSA SecurID). In addition, you can configure the Avaya VPN Gateway cluster for client certificate authentication. To test the Portal, the local database authentication method can be configured with one or several test users. For instructions on how to configure authentication methods, see Chapter 9, "Authentication Methods".

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 Chapter 11, "Group Links".

Configure Access through Net Direct Client

Net Direct eliminates the need to install VPN client software on all remote user machines. Net Direct installs a slim version of the Avaya VPN Client – the Net Direct client – when the remote user clicks the Net Direct link on the Portal's Home tab. When the user exits the session, the Net Direct client is removed from the client PC. For instructions on how to configure access using the Net Direct client, see Chapter 7, "Net Direct".

Configure Avaya Endpoint Access Control Agent

Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent, see Chapter 15, "Configure Avaya Endpoint Access Control Agent".

Customize the Portal

The Portal can be customized with respect to logo, language, color, static texts and so on. For instructions on how to customize the Portal, see Chapter 10, "Customize the Portal".

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 Chapter 16, "WholeSecurity".

HTTP to HTTPS

To configure the Avaya VPN Gateway to automatically transform an HTTP client request to the required HTTPS request, see Chapter 12, "HTTP to HTTPS Redirection".

DNS Round Robin Load Balancing

The example described in this section uses round robin load balancing performed by a DNS server. The purpose is to distribute client traffic evenly between two Avaya VPN Gateways in a cluster.

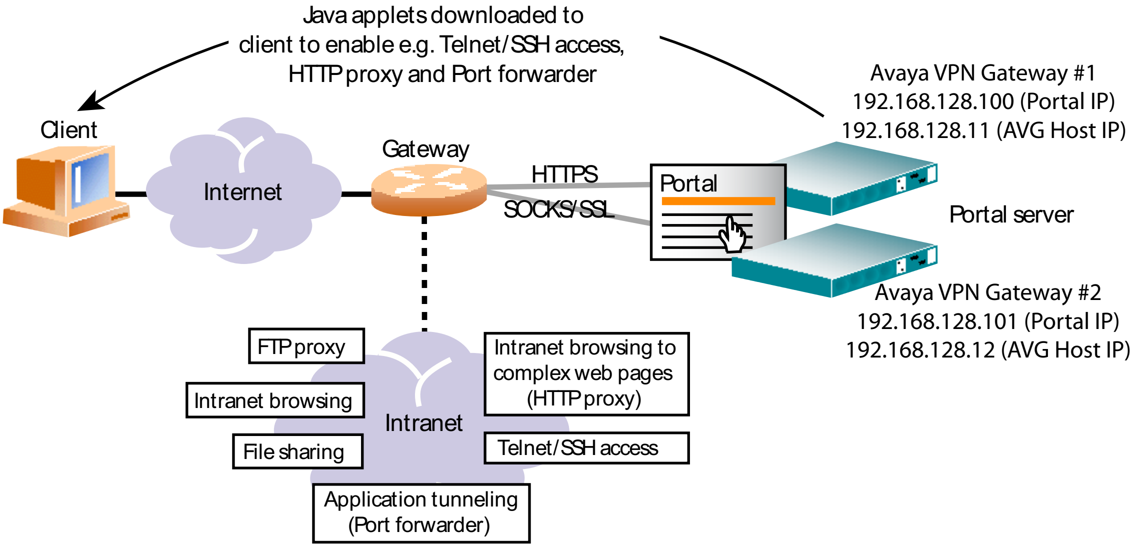

Java applets downloaded to client to enable e.g. Telnet/SSH access, HTTP proxy and Port forwarder
Client
Internet
Gateway
HTTPS
SOCKS/SSL
Portal
Avaya VPN Gateway #1
192.168.128.100 (Portal IP)
192.168.128.11 (AVG Host IP)
Portal server
Avaya VPN Gateway #2
192.168.128.101 (Portal IP)
192.168.128.12 (AVG Host IP)
FTP proxy
Intranet browsing
File sharing
Intranet
Intranet browsing to complex web pages (HTTP proxy)
Telnet/SSH access
Application tunneling (Port forwarder)

Figure 5-2 DNS Round Robin Balancing of two Avaya VPN Gateways

To realize DNS round robin load balancing, you typically add as many Portal IP addresses as there are Avaya VPN Gateways in the cluster. For instructions on how to join an Avaya VPN Gateway to an existing cluster, see the “Initial Setup” chapter in the *User’s Guide*.

In the DNS server configuration you should specify that the fully qualified domain name assigned to the Portal resolves to the Portal IP addresses configured under **VPN Gateways>VPN #>IP Addresses**. You must also configure the DNS server to perform round robin load balancing and reverse DNS lookups.

If one of the Avaya VPN Gateways in the cluster should fail, the virtual server IP address currently assigned to that Avaya VPN Gateway is migrated to another Avaya VPN Gateway in the cluster. This means that traffic directed to that IP address (by means of the DNS round robin configuration) will still reach its destination.

Add IP Addresses

1. **Log in to the BBI as administrator.**
2. **Click Config.**
3. **In system tree view, select the VPN Gateways.**

   The VPN Gateways form is displayed.
4. **Click on the VPN Gateway name.**
5. **Click on General settings in VPN Summary screen.**
6. **Click on IP Address tab.**
7. **Apply the changes.**

VPN with Application Switch

When the Avaya VPN Gateway is used for SSL acceleration, it typically requires support of an application switch for traffic redirection. With this setup, standalone mode should not be enabled. Only one (virtual) IP address (VIP) can be assigned to the portal server configured in the Avaya VPN Gateway cluster and this VIP should be mapped to the application switch.

This configuration example assumes that you have two Avaya VPN Gateways in the cluster, and that the Avaya VPN Gateways are connected to an application switch.

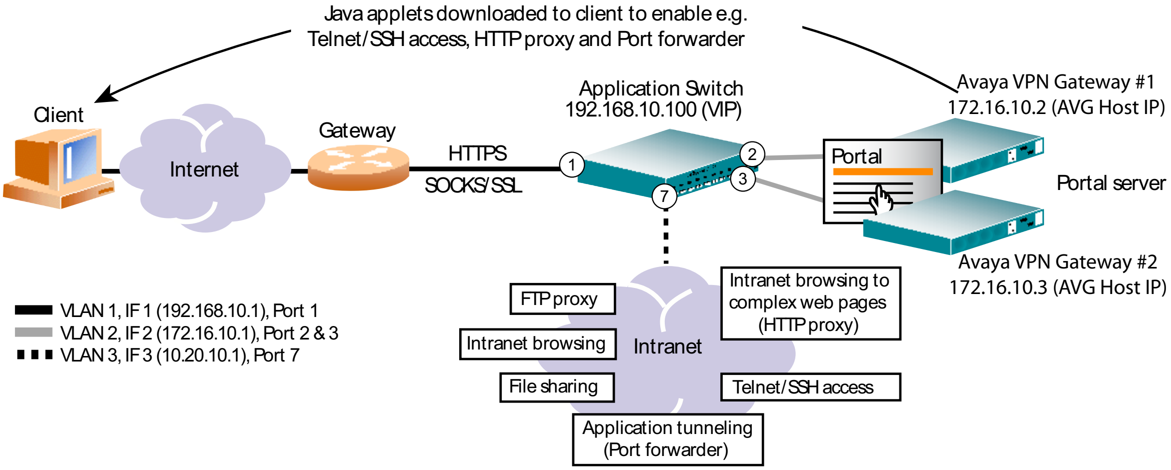

Java applets downloaded to client to enable e.g.
Telnet/SSH access, HTTP proxy and Port forwarder
Client
Internet
Gateway
HTTPS
SOCKS/SSL
Application Switch
192.168.10.100 (VIP)
1
2
3
7
Avaya VPN Gateway #1
172.16.10.2 (AVG Host IP)
Portal
Portal server
Avaya VPN Gateway #2
172.16.10.3 (AVG Host IP)
VLAN 1, IF 1 (192.168.10.1), Port 1
VLAN 2, IF 2 (172.16.10.1), Port 2 & 3
VLAN 3, IF 3 (10.20.10.1), Port 7
FTP proxy
Intranet browsing
File sharing
Intranet
Intranet browsing to complex web pages (HTTP proxy)
Telnet/SSH access
Application tunneling (Port forwarder)

Figure 5-3 VPN in Clientless Mode with Application Switch

Configure the VPN Gateway

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Click Add New VPN to create a new VPN.**

   If you would rather modify an existing VPN, go straight to Step 9

5. **In the Name field (optional), enter a name for the VPN.**

6. **In the IP address field, enter the desired IP address.**

   In the Alteon Application switch case, this IP address is called a virtual IP address (VIP). When the Avaya VPN Gateway is connected to an application switch, the VIP must also be defined on the switch. In this example, we will use **`192.168.10.100`** as the VIP.

7. **In the Certificate Number list box, select the desired server certificate.**

   The server certificate must be installed on the Avaya VPN Gateway. See the section "Import Signed Certificate to the Avaya VPN Gateway" on page 86.

8. **Click Create VPN.**

   The VPN is added to the configuration.

9. **In the System tree view, expand VPN Gateways.**

10. **Click on VPN Gateway name.**

11. **Click General settings.**

12. **Under General, set the standalone status.**

13. **Click update.**

14. **Apply the changes.**

    Next, you should configure the application switch (see next section). Among other things, the virtual IP address (VIP) that you have configured on the Avaya VPN Gateway should also be configured on the application switch.

Configure the Application Switch

Create the Necessary VLANs

In this configuration, there will be three VLANs: VLAN 1 for the Application Switch that connects to the Internet, VLAN 2 for the Avaya VPN Gateway devices, and VLAN 3 for the intranet. Because VLAN 1 is the default, only VLAN 2 and VLAN 3 requires additional configuration.

1. **Configure VLAN 2 to include Application Switch ports leading to the Avaya VPN Gateway devices.**

```
# /cfg/vlan 2
>> VLAN 2# add 2
Port 2 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# add 3
Port 3 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# ena
```

2. **Configure VLAN 3 to include the Application Switch port leading to the intranet.**

```
# /cfg/vlan 3
>> VLAN 3# add 7
Port 7 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
```

3. **Disable Spanning Tree Protocol (STP) for the Avaya VPN Gateway ports 2 and 3.**

```
# /cfg/stp/port 2
>> Spanning Tree Port 2# off
>> Spanning Tree Port 2# ../port 3
>> Spanning Tree Port 3# off
```

Configure One IP Interface for Each VLAN

NOTE – If you prefer, you can reverse the order of the first two commands (`addr` and `mask`) in the following example. By entering the mask first, the Application Switch will automatically calculate the correct broadcast address for you. The calculated broadcast address is displayed immediately after you provide the IP address of the interface, and will be applied together with the other settings when you execute the `apply` command.

1. **Configure an IP interface for client traffic on the Application Switch with VLAN 1.**

```
# /cfg/ip/if 1
>> IP Interface 1# addr 192.168.10.1
>> IP Interface 1# mask 255.255.255.0
>> IP Interface 1# broad 192.168.10.255
>> IP Interface 1# vlan 1
>> IP Interface 1# ena
```

2. **Configure an IP interface for Avaya VPN Gateway traffic with VLAN 2.**

```
# /cfg/ip/if 2
>> IP Interface 2# addr 172.16.10.1
>> IP Interface 2# mask 255.255.0.0
>> IP Interface 2# broad 172.16.255.255
>> IP Interface 2# vlan 2
>> IP Interface 2# ena
```

3. **Configure an IP interface for intranet traffic with VLAN 3.**

```
# /cfg/ip/if 3
>> IP Interface 3# addr 10.20.10.1
>> IP Interface 3# mask 255.255.255.0
>> IP Interface 3# broad 10.20.10.255
>> IP Interface 3# vlan 3
>> IP Interface 3# ena
```

4. **Apply the changes.**

```
# apply
```

NOTE – Make sure the Avaya VPN Gateways are configured to use the IP address of IP interface 2 on VLAN 2 as their default gateway. For more information about gateway configuration, see the `gateway` command under “System Configuration” in the *User’s Guide*.

Configure the Avaya VPN Gateway Load Balancing Parameters

Set and enable the IP addresses of the Avaya VPN Gateways, and create a group in the switch for load balancing.

1. **Define each Avaya VPN Gateway as a real server and specify the real server IP address.**

   The real server IP (RIP) address you are asked to specify in this case is the IP address you assigned to each Avaya VPN Gateway during the initial setup. To view the real IP address of each Avaya VPN Gateway in the cluster, you can use the `/info/isdlist` command

```
# /cfg/slb/real 1
>> Real server 1# rip 172.16.10.2
>> Real server 1# ena
>> Real server 1# ../real 2
>> Real server 2# rip 172.16.10.3
>> Real server 2# ena
```

2. **Create a real server group and add the real servers (the Avaya VPN Gateways in this case) to the group.**

```
# /cfg/slb/group 1
>> Real server group 1# add 1
>> Real server group 1# add 2
```

3. **Set the load balancing metric and health check type for real server group 1.**

```
# /cfg/slb/group 1
>> Real server group 1# metric hash
>> Real server group 1# health sslh
```

4. **Set and enable the IP address for Virtual Server 1, enable service on port 443, and assign server group 1 (the Avaya VPN Gateways) to this service**.

   The reason for configuring a virtual server is solely to ensure that the application switch will respond to the ARP request for the virtual IP address (VIP). Server load balancing cannot be used with Avaya VPN Gateway because the Portal IP address must be preserved as destination IP address in the TCP packets. Instead, a redirect filter is used (see “Configure Redirect Filters” on page 104).

```
# /cfg/slb/virt 1
>> Virtual Server 1# vip 192.168.10.100
>> Virtual Server 1# ena
>> Virtual Server 1# service https
>> Virtual Server 1 https Service# group 1
```

5. **Enable client processing on port 1 leading to the Internet.**

```
# /cfg/slb/port 1
>> SLB Port 1# client ena
```

6. **Turn on Layer 4 processing.**

```
# /cfg/slb/on
```

7. **Apply the changes.**

```
# apply
```

Configure Redirect Filters

1. **Create a filter to redirect client HTTPS traffic intended for port 443 on the Virtual Server IP (VIP) address.**

   When this filter is added to the switch port leading to the Internet, incoming HTTPS traffic destined for the virtual server IP address is redirected to the Avaya VPN Gateways in real server group 1.

```
# /cfg/slb/filt 100
>> Filter 100# dip 192.168.10.100
>> Filter 100# dmask 255.255.255.255
>> Filter 100# proto tcp
>> Filter 100# dport https
>> Filter 100# action redir
>> Filter 100# group 1
>> Filter 100# rport https
>> Filter 100# ena
```

2. **Create a default filter to allow all other traffic.**

```
# /cfg/slb/filt 224
>> Filter 224# sip any
>> Filter 224# dip any
>> Filter 224# proto any
>> Filter 224# action allow
>> Filter 224# ena
```

CHAPTER 6

The Portal from an End-User Perspective

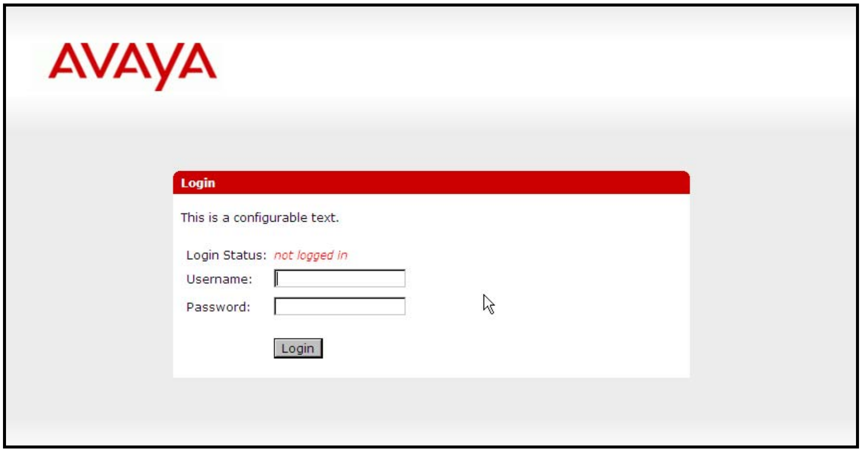
This chapter describes the Portal from a user perspective. It includes step-by-step instructions on how access intranet resources in clientless mode, for example through the Portal. For instructions on how to change the Portal's look and feel, see Chapter 10, "Customize the Portal".

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.

1. **In the available web browser, the remote user should enter the domain name (for example, https://vpn.example.com) or IP address (for example, https://192.168.128.100) to the Avaya VPN Gateway.**

The Portal login page is displayed:



This is a configurable text.

Login Status: *not logged in*

Username:

Password:

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 Avaya VPN Gateway's local authentication database or in an external authentication database (for example RADIUS, LDAP, CA SiteMinder, NTLM, RSA SecurID or RSA ClearTrust).

   NOTE – If using a secondary authentication method, an extra password field displays. The first field (Passcode) authenticates the primary authentication scheme and the second field (Password) authenticates the secondary authentication scheme You must use the same username with both the primary and secondary authentication through the SSL portal. 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 a certificate authentication server automatically supports IPsec two factor authentication. In IPsec Two Factor authentication the client must provide both the username and password to the requesting server. IPsec Two Factor Authentication supports only certificate authentication as primary and local, RADIUS or LDAP as secondary.

   Configuring authentication methods is described in Chapter 9, "Authentication Methods".

2. **To direct the remote user to a specific authentication database (if several different authentication methods are configured for the Avaya VPN Gateway), 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 #>Authentication>(Method)>General** form and enter the desired name in the **Display Name** field (also see Chapter 9, “Authentication Methods”).

NOTE – If no display name has been configured for any of the authentication methods used, the Login Service list box will not be displayed.

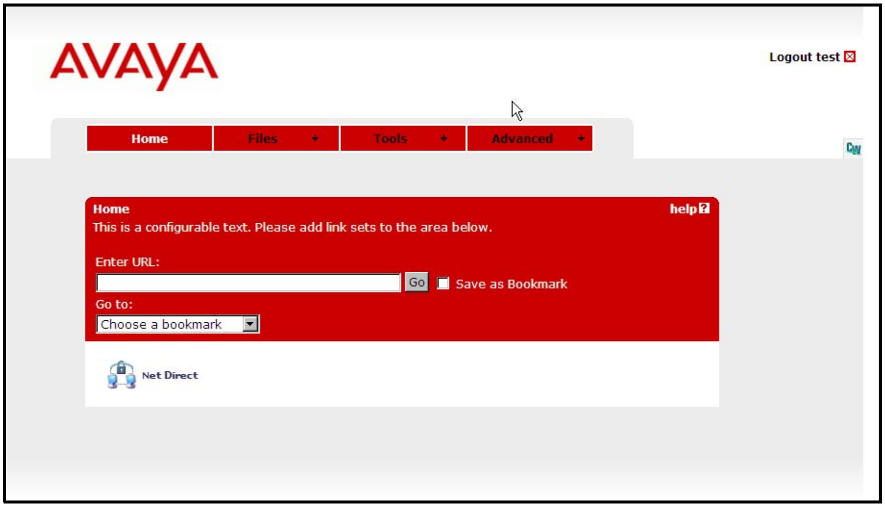
---

3. **Click Login.**

   The Portal web page is displayed.

The Portal Web Page

Once the user is successfully authenticated, the Portal web page is displayed.



This is a configurable text. Please add link sets to the area below.

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 Chapter 8, “Groups, Access Rules and Profiles”.

The Portal’s look and feel can be customized with respect to language, logo, company name, colors and static text (see Chapter 10, “Customize the Portal”).

The icons to the right of the Portal tabs indicate whether or not certain Java applets and ActiveX controls are active.

Avaya Endpoint Access Control Agent

Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent, see Chapter 15, “Configure Avaya Endpoint Access Control Agent”.

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 Avaya 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 Chapter 11, “Group Links” for instructions. Citrix Metaframe support is disabled by default (see **VPN Gateways>VPN #>Portal Display>General**).

IE Cache Wiper

The IE Cache Wiper is an ActiveX control that clears the cache (visited URLs and cached HTML documents) after a Portal session for users running Internet Explorer. The IE Cache Wiper is enabled by default (see **VPN Gateways>VPN #>Portal Display>General**).

Net Direct Client

The Net Direct client is a VPN client similar to the Avaya 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 Avaya VPN Gateway for use with the Net Direct client, see Chapter 7, “Net Direct”.

Capabilities

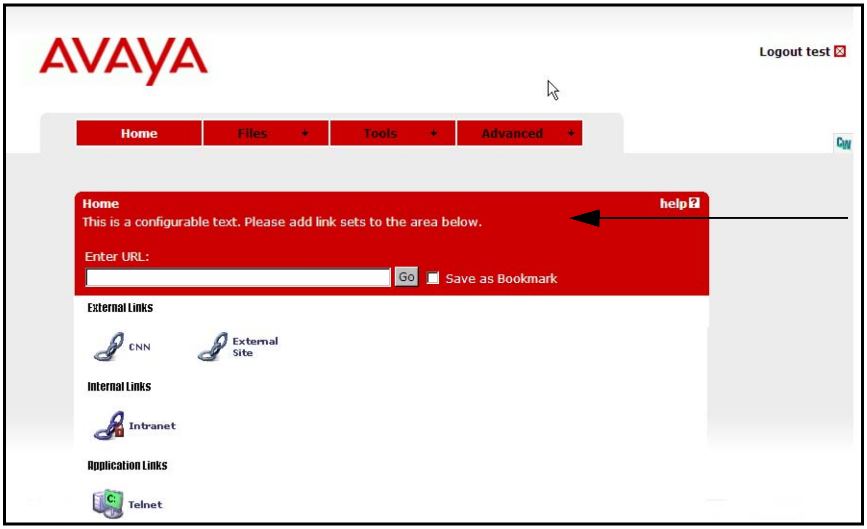
In clientless mode, the following services are enabled:

- 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 using a well-defined set of ports) through SOCKS encapsulated in SSL.
- 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.



This is a configurable text. Please add link sets to the area below.

How to configure this text is described in Chapter 10, “Customize the Portal”.

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 Avaya VPN Gateway as e.g. http://inside.example.com. A new browser window is opened, but now the request is rewritten with the Avaya VPN Gateway rewrite prefix (boldface) added, e.g. **https://vpn.example.com**/http/inside.example.com. This way, traffic is secured by the Avaya VPN Gateway.

Visited URLs can be saved as bookmarks by selecting the **Save as Bookmark** check box before clicking **Go** (see page 114 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 links are:

- Secure link (through Avaya VPN Gateway) or direct link to web page
- Secure automatic logon link (through Avaya VPN Gateway) to password-protected web page

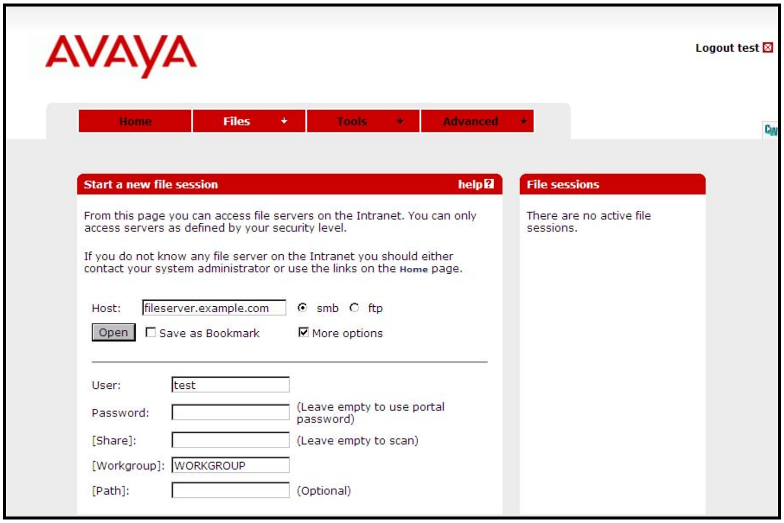
- Link to FTP or SMB file server
- Application tunnel link (port forwarder) through SOCKS encapsulated in SSL
- HTTP Proxy link (ensures display of web pages linked through plugins, e.g Flash)
- Link to Telnet or SSH terminal servers
- Net Direct link (downloads the Net Direct client)

See Chapter 11, “Group Links” for instructions on how to configure Portal links.

NOTE – The **Download** tab in the Portal will be available only when the SPO access is enabled.

The Files Tab

The Files tab lets the user access a remote SMB (Windows file share) or FTP file server.



Start a new file session

From this page you can access file servers on the Intranet. You can only access servers as defined by your security level.

If you do not know any file server on the Intranet you should either contact your system administrator or use the links on the Home page.

Host: fileserver.example.com ● smb ○ ftp

□ Save as Bookmark ☑ More options

User: test

Password: (Leave empty to use portal password)

[Share]: (Leave empty to scan)

[Workgroup]: WORKGROUP

[Path]: (Optional)

File sessions

There are no active file sessions.

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, i.e. 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.**

5. **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.

6. **To make the file server accessible through a Bookmark (selectable from the Home tab), select Save as Bookmark.**

   For a more detailed explanation of the Save as Bookmark option, see page 114.

7. **Click Open.**

   Files and folders contained in the specified folder are displayed by file type icon, file name, size, and date.

   Note: 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 #>Single Sign-On>SSO Domains and Headers.

   - 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.

NOTE – The **Download** tab in the Portal will be available only when the SPO access is enabled.

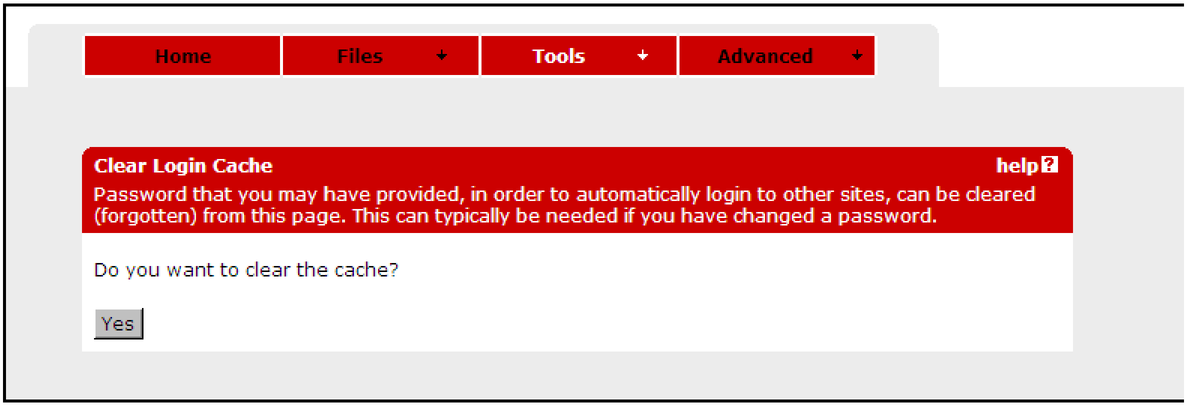
The Tools Tab, System Information

To view information about the current version of the Avaya VPN Gateway 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 form 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 Avaya VPN Gateway system's cache from any kind of login information supplied during a Portal session.



Clear Login Cache

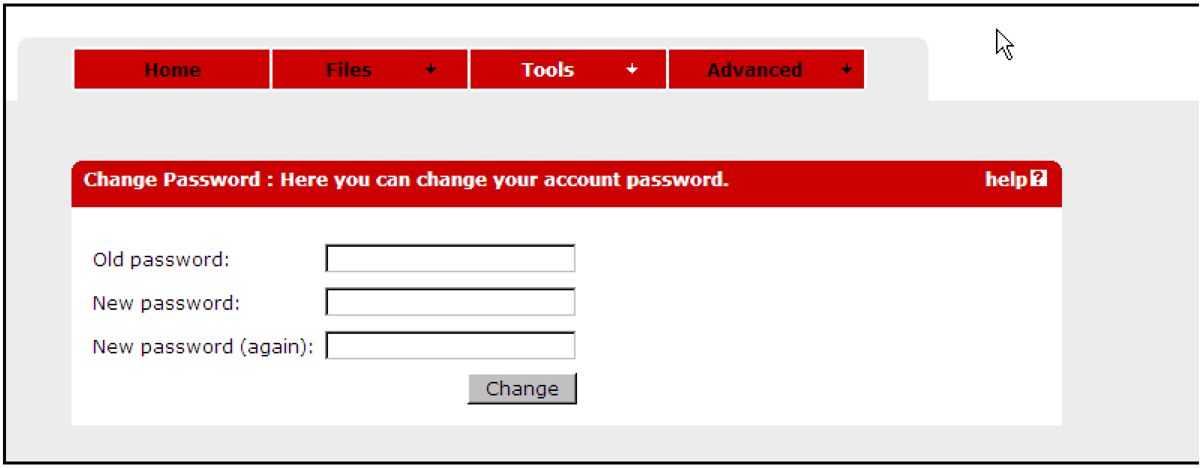
Password that you may have provided, in order to automatically login to other sites, can be cleared (forgotten) from this page. This can typically be needed if you have changed a password.

Do you want to clear the cache?

Yes

The Tools tab, Change User Password

The **Change Password** option on the **Tools** submenu lets the remote user change his Portal password.



Change Password : Here you can change your account password.

Old password:

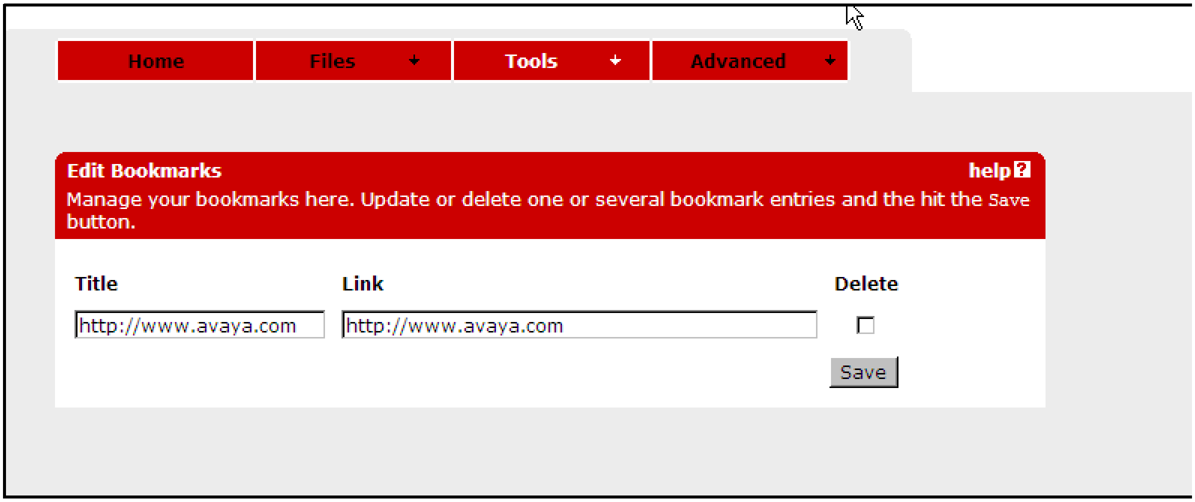
New password:

New password (again):

Note that this only applies if the user has logged in through the local database authentication method, i.e. has his/her password stored in the Avaya 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.



Edit Bookmarks

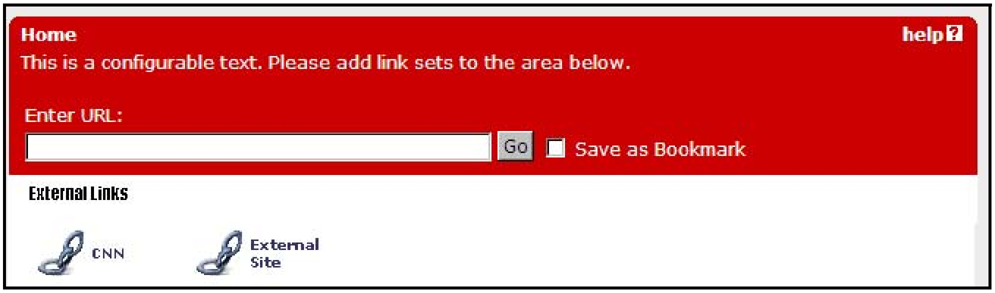
Manage your bookmarks here. Update or delete one or several bookmark entries and the hit the Save button.

Title	Link	Delete
http://www.avaya.com	http://www.avaya.com	□

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> VPN #>Authentication>LDAP>LDAP Settings** in the BBI. You should also add the *isdUserPrefs* attribute to Active Directory (see Appendix H in the *User's Guide* for instructions).

Saved bookmarks can later be selected in the **Go to** list box on the Portal's Home tab:



Home

This is a configurable text. Please add link sets to the area below.

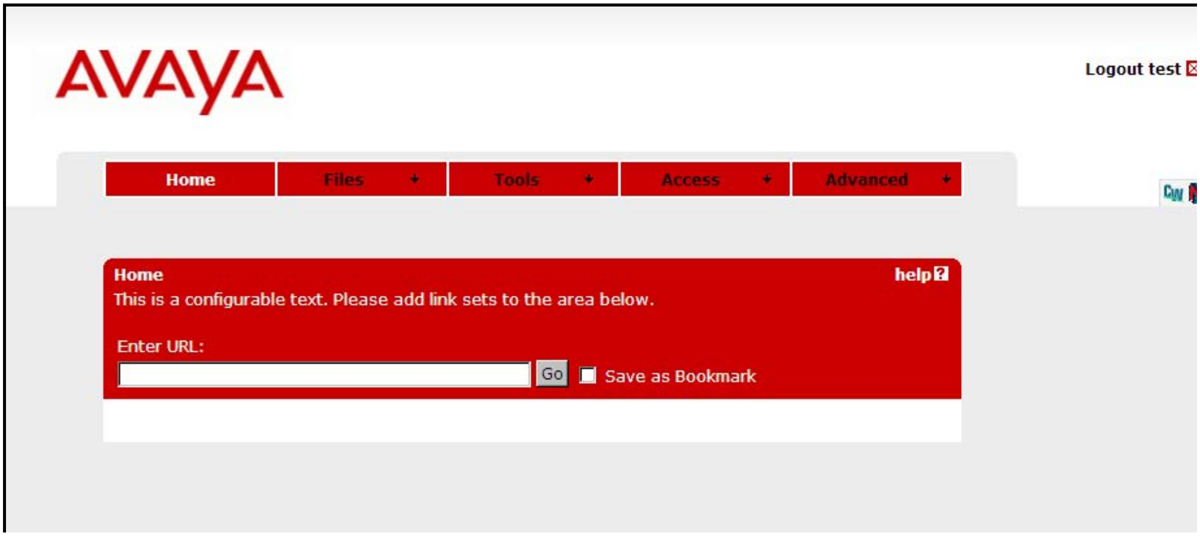
Enter URL:

NOTE – The **Download** tab in the Portal will be available only when the SPO access is enabled.

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, i.e. no (further) Portal interaction is required. Supported VPN clients are the Avaya VPN Client and the Net Direct client.



This is a configurable text. Please add link sets to the area below.

Enter URL:

□ Save as Bookmark

The **Access** tab is not displayed on the Portal by default, nor is VPN client access enabled by default. Follow the instructions in Chapter 21, “Transparent Mode” and Chapter 7, “Net Direct” respectively to enable access to the VPN from the **Access** tab, using the Avaya VPN Client and/or the Net Direct client.

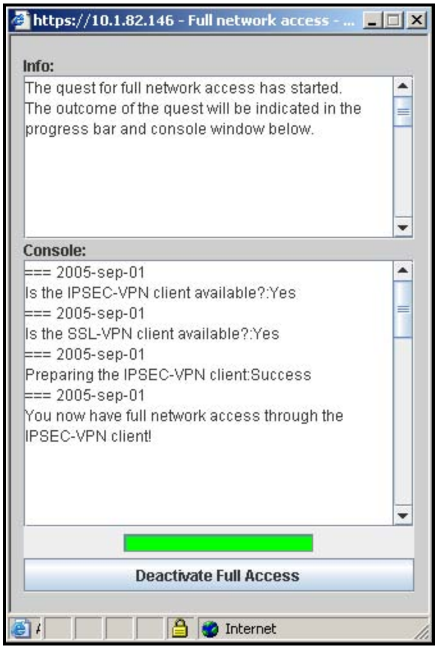
To start a VPN client from the Access tab, the user should do the following:

1. **Click the Yes button.**

   A Java applet is downloaded to the user’s local machine. The Java applet checks if the Avaya VPN Client is installed and able to connect to an Avaya VPN Router or to the Avaya VPN Gateway. If so, the Avaya VPN Client is silently activated on the remote user’s machine.

If the Avaya 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 Avaya 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/Avaya VPN Gateway.



The quest for full network access has started.
The outcome of the quest will be indicated in the progress bar and console window below.

```
=== 2005-sep-01
Is the IPSEC-VPN client available?:Yes
=== 2005-sep-01
Is the SSL-VPN client available?:Yes
=== 2005-sep-01
Preparing the IPSEC-VPN client:Success
=== 2005-sep-01
You now have full network access through the
IPSEC-VPN client!
```

This is an example of the Java applet window when a connection to the Avaya VPN Gateway is successfully established with the Avaya VPN Client.

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.

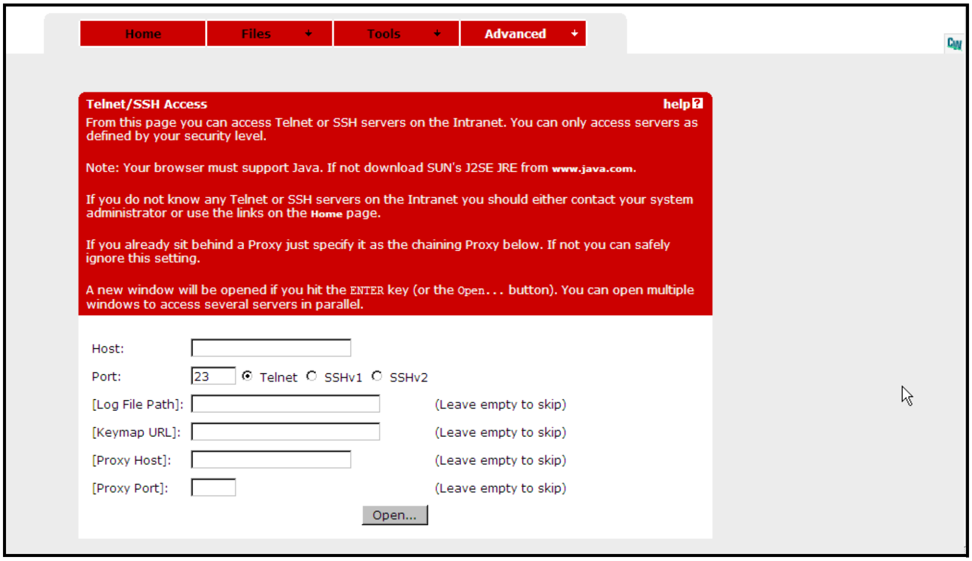
   If neither of the VPN clients are installed or able to connect, intranet resources can only be accessed in *clientless mode*, i.e. by requesting resources from the other Portal tabs.

NOTE – The **Download** tab in the Portal will be available only when the SPO access is enabled.

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.



Telnet/SSH Access

From this page you can access Telnet or SSH servers on the Intranet. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from **www.java.com**.

If you do not know any Telnet or SSH servers on the Intranet you should either contact your system administrator or use the links on the **Home** page.

If you already sit behind a Proxy just specify it as the chaining Proxy below. If not you can safely ignore this setting.

A new window will be opened if you hit the `ENTER` key (or the `Open...` button). You can open multiple windows to access several servers in parallel.

Host:		
Port:	23 ● Telnet ○ SSHv1 ○ SSHv2	
[Log File Path]:		(Leave empty to skip)
[Keymap URL]:		(Leave empty to skip)
[Proxy Host]:		(Leave empty to skip)
[Proxy Port]:		(Leave empty to skip)

Open...

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 Appendix F, “Definition of Key Codes” in the *User’s Guide*.

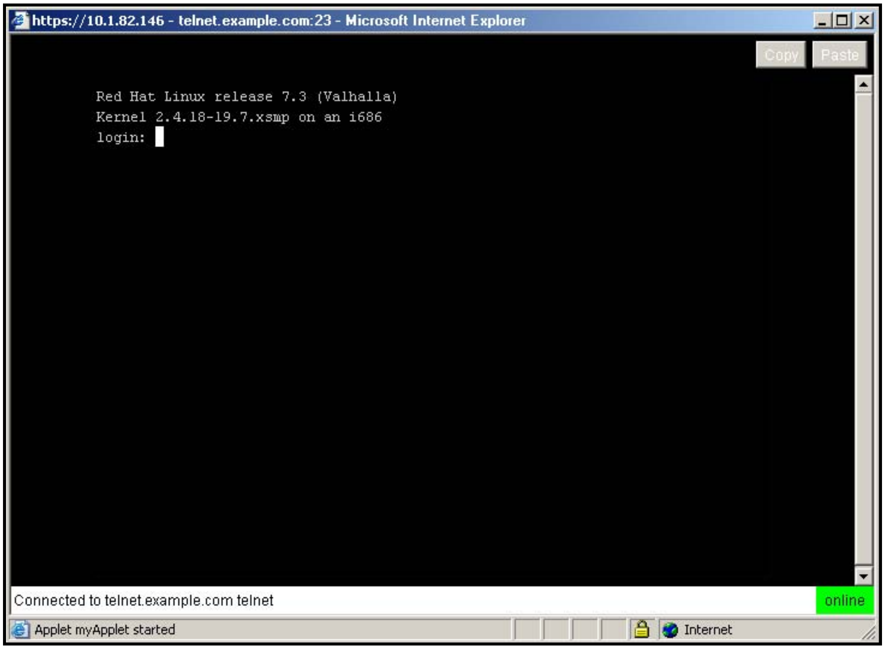
5. **In the [Proxy Host] and [Proxy Port] fields, enter the IP address and port number of an intermediate Proxy server (if any).**

   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 Avaya 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 Avaya VPN Gateway.

6. **Click Open.**

   This is what the Java applet window might look like when a Telnet session is started:



https://10.1.82.146 - telnet.example.com:23 - Microsoft Internet Explorer
Copy
Paste

```
Red Hat Linux release 7.3 (Valhalla)
Kernel 2.4.18-19.7.xsmp on an i686
login:
```

Connected to telnet.example.com telnet
online
Applet myApplet started
Internet

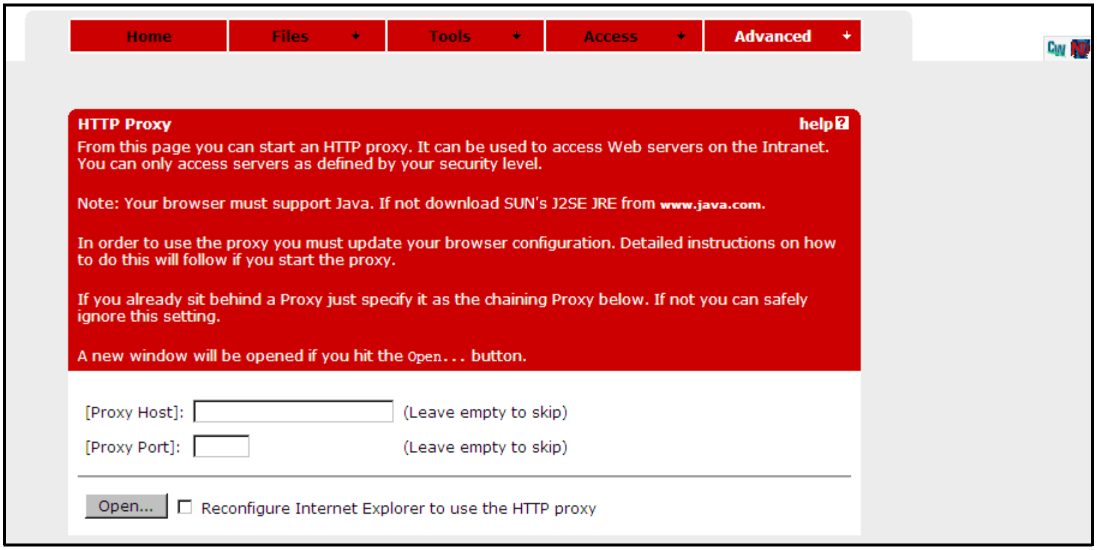
7. **Click in the window to activate it before logging in to the terminal session.**

   To quit the session, exit the terminal session and click the Close button top right.

he 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 Avaya 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 Avaya VPN Gateway’s proxy server, where it is unpacked and redirected to its proper destination.



HTTP Proxy

From this page you can start an HTTP proxy. It can be used to access Web servers on the Intranet. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from **www.java.com**.

In order to use the proxy you must update your browser configuration. Detailed instructions on how to do this will follow if you start the proxy.

If you already sit behind a Proxy just specify it as the chaining Proxy below. If not you can safely ignore this setting.

A new window will be opened if you hit the `Open...` button.

[Proxy Host]: (Leave empty to skip)

[Proxy Port]: (Leave empty to skip)

Open... □ Reconfigure Internet Explorer to use the HTTP proxy

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 Avaya 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 Avaya VPN Gateway.

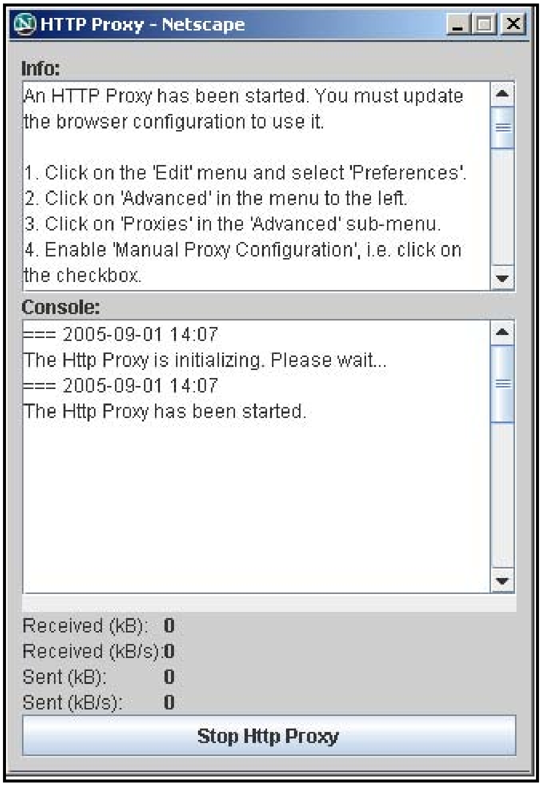
2. **If Internet Explorer is used as the client browser, the user may select the check box Reconfigure Internet Explorer to use the HTTP Proxy.**

   With this check box selected, the user does not have to change the browser's proxy settings manually, i.e. 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).**



Info:

An HTTP Proxy has been started. You must update the browser configuration to use it.

1. Click on the 'Edit' menu and select 'Preferences'.
2. Click on 'Advanced' in the menu to the left.
3. Click on 'Proxies' in the 'Advanced' sub-menu.
4. Enable 'Manual Proxy Configuration', i.e. click on the checkbox.

Console:

```
=== 2005-09-01 14:07
The Http Proxy is initializing. Please wait...
=== 2005-09-01 14:07
The Http Proxy has been started.
```

Received (kB): 0
Received (kB/s): 0
Sent (kB): 0
Sent (kB/s): 0

Unless Internet Explorer is used as client browser (see Step 2), the browser'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 Avaya VPN Gateway's HTTP Proxy. The Java applet window and the Portal session must be active.

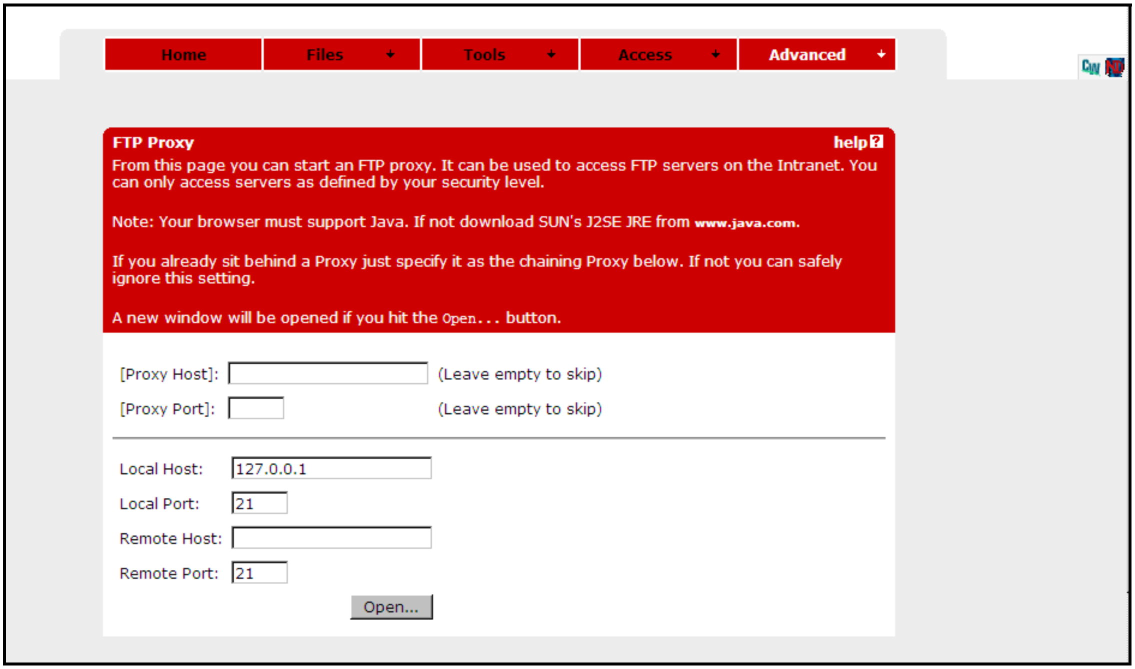
To quit the HTTP Proxy session, the user should click the Stop Http Proxy button in the Java applet window. If the browser was reconfigured manually, the user should also change the browser settings back to the original settings.

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 Avaya VPN Gateway's proxy server, where it is relayed to the specified FTP server.



FTP Proxy help

From this page you can start an FTP proxy. It can be used to access FTP servers on the Intranet. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from www.java.com.

If you already sit behind a Proxy just specify it as the chaining Proxy below. If not you can safely ignore this setting.

A new window will be opened if you hit the Open... button.

[Proxy Host]: (Leave empty to skip)

[Proxy Port]: (Leave empty to skip)

Local Host: 127.0.0.1

Local Port: 21

Remote Host:

Remote Port: 21

Open...

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 Avaya 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 Avaya 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 (i.e. `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 Step 2.

8. **To quit the FTP Proxy, the user should click the Stop FTP Proxy button in the Java applet window.**

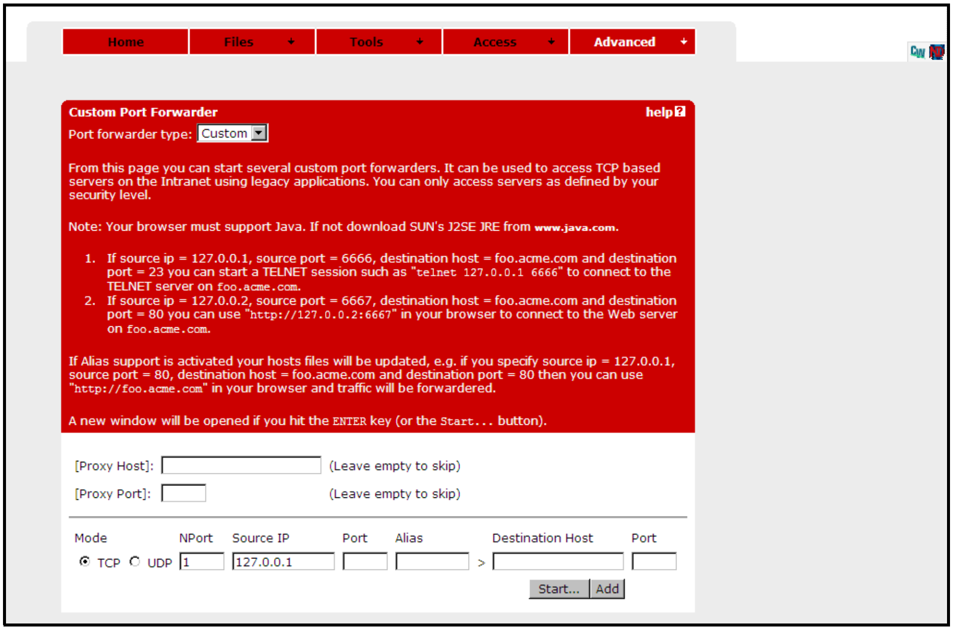
The Advanced Tab, Port Forwarders

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.



Custom Port Forwarder help

Port forwarder type: Custom

From this page you can start several custom port forwarders. It can be used to access TCP based servers on the Intranet using legacy applications. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from www.java.com.

1. If source ip = 127.0.0.1, source port = 6666, destination host = foo.acme.com and destination port = 23 you can start a TELNET session such as "`telnet 127.0.0.1 6666`" to connect to the TELNET server on `foo.acme.com`.
2. If source ip = 127.0.0.2, source port = 6667, destination host = foo.acme.com and destination port = 80 you can use "`http://127.0.0.2:6667`" in your browser to connect to the Web server on `foo.acme.com`.

If Alias support is activated your hosts files will be updated, e.g. if you specify source ip = 127.0.0.1, source port = 80, destination host = foo.acme.com and destination port = 80 then you can use "`http://foo.acme.com`" in your browser and traffic will be forwardered.

A new window will be opened if you hit the `ENTER` key (or the `Start...` button).

[Proxy Host]: (Leave empty to skip)

[Proxy Port]: (Leave empty to skip)

Mode	NPort	Source IP	Port	Alias		Destination Host	Port
● TCP ○ UDP	1	127.0.0.1			>		

Start... Add

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 Avaya 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 Avaya VPN Gateway.

2. **Under Mode, select the desired packet transfer protocol, i.e. 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`.

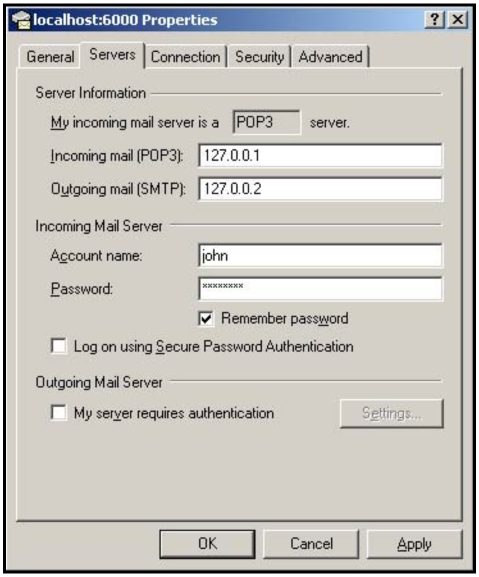
   Up to 16 tunnels can be created for one port forwarder.

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.



Server Information

My incoming mail server is a POP3 server.

Incoming mail (POP3): 127.0.0.1

Outgoing mail (SMTP): 127.0.0.2

Incoming Mail Server

Account name: john

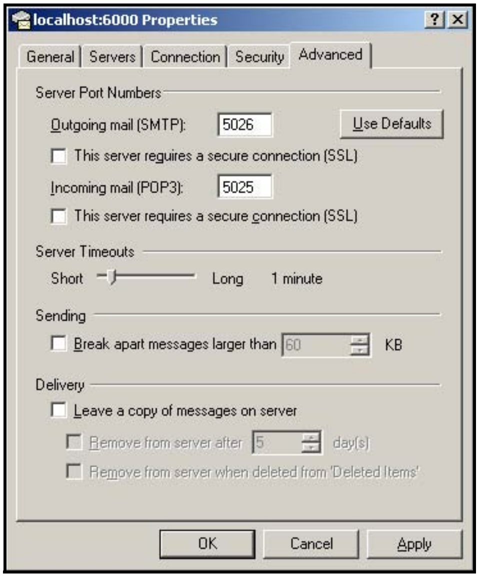
Password: ********

☑ Remember password

☐ Log on using Secure Password Authentication

Outgoing Mail Server

☐ My server requires authentication



Server Port Numbers

Outgoing mail (SMTP): 5026

☐ This server requires a secure connection (SSL)

Incoming mail (POP3): 5025

☐ This server requires a secure connection (SSL)

Server Timeouts

Short Long 1 minute

Sending

☐ Break apart messages larger than 60 KB

Delivery

☐ Leave a copy of messages on server

☐ Remove from server after 5 day(s)

☐ Remove from server when deleted from 'Deleted Items'

The port numbers to use are the ones entered in the “local” **Port** field for the POP3 and SMTP servers respectively, i.e. `5025` and `5026`. By entering the application-specific port numbers in the “local” **Port** field, i.e. `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.

If you expect the connection to include more than 15 minutes of inactivity, increase the **Client TCP Keep Alive Timeout** value in the BBI (under **VPN Gateways>VPN # >TCP**).

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

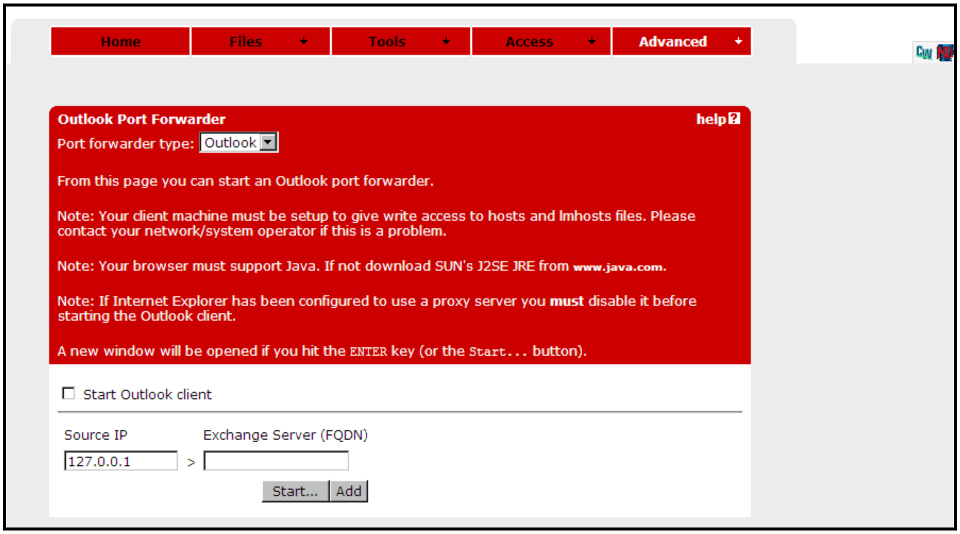
To establish a secure HTTP session using the Custom Port Forwarder, proceed as described, only enter the host address to the Web server in the **Destination Host** field and port number `80` in the "remote" **Port** field instead. The user can then start his or her browser and type for example `127.0.0.1:5025` 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 Avaya VPN Gateway operator. A Custom Port forwarder link can be defined to launch the application automatically (see Chapter 11, "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:



Outlook Port Forwarder

Port forwarder type: Outlook

From this page you can start an Outlook port forwarder.

Note: Your client machine must be setup to give write access to hosts and lmhosts files. Please contact your network/system operator if this is a problem.

Note: Your browser must support Java. If not download SUN's J2SE JRE from www.java.com.

Note: If Internet Explorer has been configured to use a proxy server you **must** disable it before starting the Outlook client.

A new window will be opened if you hit the `ENTER` key (or the `Start...` button).

□ Start Outlook client

Source IP		Exchange Server (FQDN)
127.0.0.1	>	

Start... Add

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 #>DNS>Search List**). 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 Avaya 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.
- 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 Avaya 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.
- If you expect the connection to include more than 15 minutes of inactivity, increase the **Client TCP Keep Alive Timeout** value in the BBI (under **VPN Gateways> VPN #>TCP**).

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, e.g. `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.

Port Forwarder API

The Avaya VPN Gateway 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.**

   Instructions for how to create Port forwarder links in Chapter 11, "Group Links".

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/nortel_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*.

The Download Tab

To download the Secure Portable Office (SPO) software images, click on **Download** tab.

By clicking the links, SPO client downloads ISO image, U3P package, and MSI files.The **Download** tab will be available in the portal only when the SPO access is enabled.

Logging out from the Portal

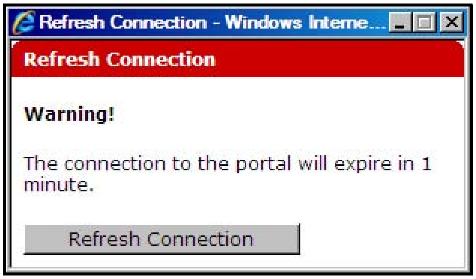
To logout from the Portal, the user should click the **Logout** prompt or the exit button top right.

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 #>Session**), the user will be logged out automatically. Note that session idle time can also be specified on group level (under **VPN Gateways>VPN #>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 #>Session**), irrespective of the user being idle or not. Note that maximum session length can also be specified on group level (under **VPN Gateways>VPN #>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.



Refresh Connection

Warning!

The connection to the portal will expire in 1 minute.

IE Cache Wiper

For users running Internet Explorer, any HTML pages that have been accessed through the Portal will be cleared from the cache, provided the IE Cache Wiper has been downloaded. The user has the option to download the IE Cache Wiper when logging in to the Portal, if the **Use**

ActiveX Component For Clearing Cache setting (under **VPN Gateways>VPN #>Portal Display>General**) is enabled (enabled by default). The IE Cache Wiper also clears the browser history from entries accumulated during the Portal session. Previously recorded entries remain.

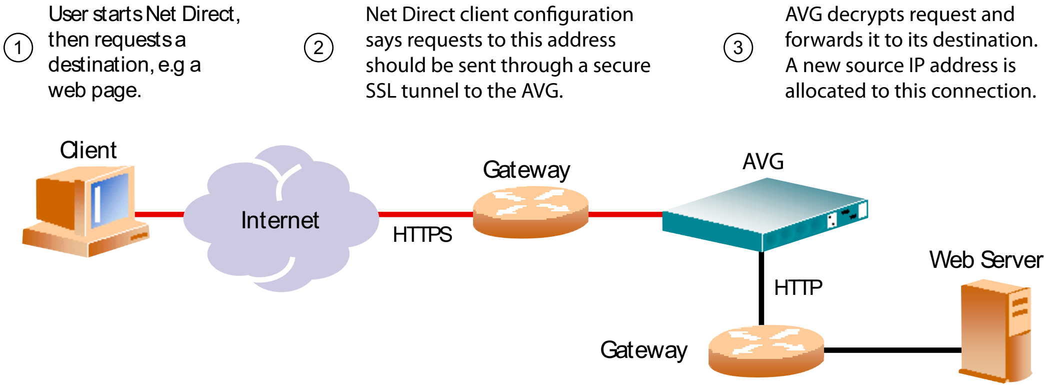
If desired, the IE Cache Wiper can be enabled/disabled on group level instead of VPN level. Set **Use ActiveX Component For Clearing Cache** to `group`, then enable or disable the **Wiper** setting under **VPN Gateways>VPN #>Group Settings>Groups>General**.

CHAPTER 7
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 client is packet-based that includes a network driver that captures network traffic and tunnels it through SSL to the Avaya VPN Gateway. The Avaya VPN Gateway then decrypts the traffic and forwards it to the requested configured tunneled network destination. Because the Net Direct client thus operates on a lower network level, it supports more applications, e.g. Microsoft Outlook and the ability to map network drives.



1 User starts Net Direct, then requests a destination, e.g a web page.

2 Net Direct client configuration says requests to this address should be sent through a secure SSL tunnel to the AVG.

3 AVG decrypts request and forwards it to its destination. A new source IP address is allocated to this connection.

Figure 7-1 Net Direct Client Connection

Supported Operating Systems

Net Direct is supported on the Windows, Linux, Intel Mac, and Mac OS X (for PowerPC) operating systems.

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 Windows administrator user name and password can however be stored on the Avaya VPN Gateway on a per group level. For remote users who are members of a group for which a valid Windows administrator user name and password have been stored, downloading and installing Net Direct is seamless. See "Configure Windows Administrator User Name/Password" on page 158.

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 limitations, supported browsers and Java versions.

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 page 150, beginning with Step 13.

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 behavior of the installable version of Net Direct is completely controlled by the server settings made for the Avaya 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 160.

When connecting to the Avaya VPN Gateway, 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 Net Direct user session, the Net Direct 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 Net Direct 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 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 is supported on Windows, Linux and MAC. It is also supported on portal version of Net Direct as well as NDIC.

Net Direct Connections

The route table monitoring logic ignores the route table changes that do not affect the Net Direct tunnel. If a user manually adds a route using the Net Direct device or deletes a route that was set up by Net Direct, then it disconnects and reconnects, cleaning up any unwanted route table entries in the process.

The Net Direct changes does not get affected even in the following scenarios:

- Physical link up/down
- RIP or similar service startup/shutdown
- VPN client connecting and setting up its own routes.

NOTE – This behavior is enabled by default.

If you want to ignore all route changes and keep Net Direct connected, you need to disable route table monitoring all together.

This is supported on Windows, Linux and MAC. It will also work for portal version of Net Direct as well as NDIC.

When the Net Direct client starts, it checks with the server if route table monitoring is enabled or disabled.

If route table monitoring is enabled, it will create a list of destinations that it wants to be routed through the Net Direct tunnel. When a new route is added or deleted, the destination of the new route is checked against the list.

- If the destination falls outside of the list, the route change is ignored.
- If the destination falls within one of the subnets in the list, then Net Direct invokes the current logic of disconnecting and reconnecting automatically.

When split tunneling is disabled, then user cannot see any marked improvement because all route changes are significant in this mode.

When split tunneling is enabled, then any route change that does not affect the tunnel is ignored. This includes changes due to the following reasons:

- User manually adding/deleting routes
- Start up of a system service like RIP that updates the routing table
- Link up/down on one of the NICs present in the system (including the NIC through which Net Direct is communicating)

There is a special case where the IP address of AVG is part of the split net configuration.

For example, consider an AVG with IP address 47.80.18.1 and with split net configured as 47.0.0.0/8. In this case, there will be a route to 47.80.18.1 through the physical interface. When the physical interface goes down, this route is deleted by the OS. But this will not disconnect even though the 47.80.18.1 destination is part of the split net configuration.

If route table monitoring is disabled, then Net Direct client disables its route monitoring logic. In this case, user can add static routes through the Net Direct tunnel to reach internal hosts that are not allowed by the split net configuration.

Note: If the administrator wants to prevent this, then it has to be enforced by defining appropriate access lists.

Server Configuration

To enable usage of the Net Direct client, follow the basic instructions in Chapter 5, “Clientless Mode” on how to set up a VPN. Once completed, continue with the instructions in the following sections.

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 Avaya VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

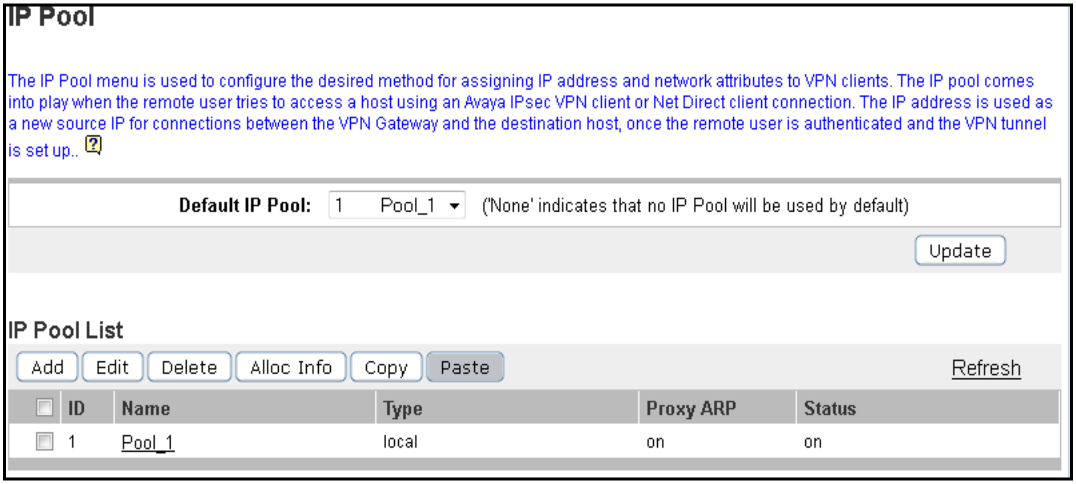
Several IP Pools can be configured, each with a unique ID number and unique properties. By mapping the desired IP Pool to a user group, you can create different methods for IP address and network attributes assignment for different user groups.

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 VPN Client) as well (see Chapter 21, “Transparent Mode”). If you have already configured an IP Pool for use with the Avaya VPN Client, this pool can also be used for the Net Direct client.

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on IP Pool settings.**

   The IP Pool form is displayed.



IP Pool

The IP Pool menu is used to configure the desired method for assigning IP address and network attributes to VPN clients. The IP pool comes into play when the remote user tries to access a host using an Avaya IPsec VPN client or Net Direct client connection. The IP address is used as a new source IP for connections between the VPN Gateway and the destination host, once the remote user is authenticated and the VPN tunnel is set up..

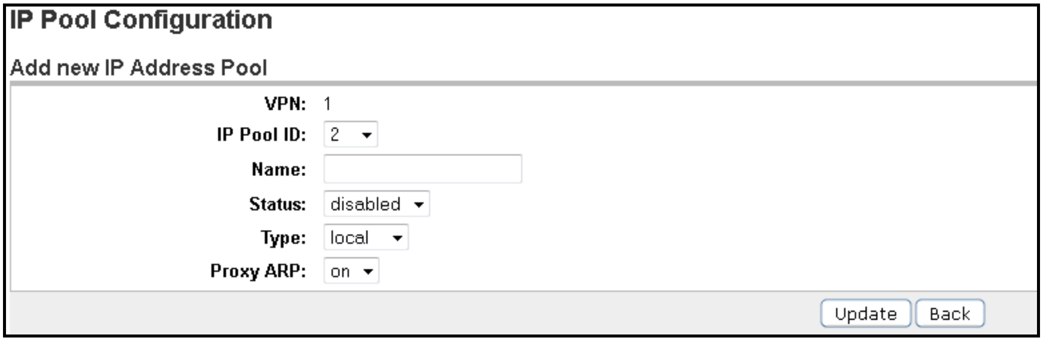
Default IP Pool: 1 Pool_1 ▾ ('None' indicates that no IP Pool will be used by default)

IP Pool List

☐	ID	Name	Type	Proxy ARP	Status
☐	1	Pool_1	local	on	on

5. **Specify a previously created IP Pool number.**
   This IP Pool will be the default IP Pool for the VPN, that is its settings will be used when no IP Pool is specified for a specific user group in the VPN. The IP Pool governs how IP addresses and network attributes are assigned to IPsec client connections and Net Direct client connections.
6. **Gives the user the ability to set the number of IP Pools for each VPN.**
   By default the number of IP Pools for each VPN is set as 30. In order to increase the number of IP Pools for a given VPN beyond 30, this value needs to be set. But the total number of IP Pools across all VPNs can only be 1024.
7. **Under IP Pool List, click Add.**

The IP Pool Configuration form is displayed.



IP Pool Configuration

Add new IP Address Pool

VPN:	1
IP Pool ID:	2
Name:	
Status:	disabled
Type:	local
Proxy ARP:	on

The first available IP Pool number is suggested in the IP Pool ID list box.

8. **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.

9. **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.

10. **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 (from the Avaya VPN Gateway), from an external RADIUS server or from an external DHCP server.

    For IP Pools of the `local` type, network attributes should be configured on the Avaya VPN Gateway (see next section). For IP Pools of the `radius` and `dhcp` types, network attributes can be configured on the Avaya VPN Gateway as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute.

11. **If needed, change the default proxy ARP setting.**

    `on`: Means that the Avaya 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 Avaya 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.

12. **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 following description depending on your choice.

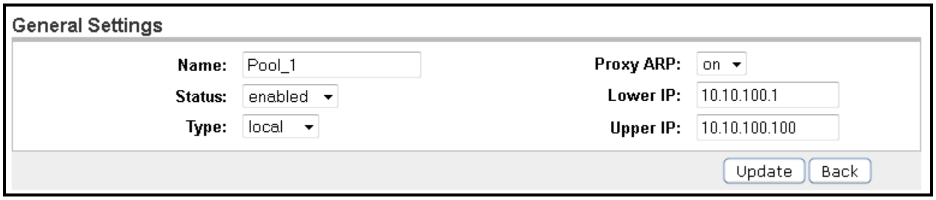
    You can associate an Internet Protocol (IP) Pool with a particular host in a clustered environment. For more information about creating an Host IP Pool, see "Create Host IP Pool" on page 143.

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism to `local` (as described in Step 10 in the previous section), you should configure the desired IP address range. You can also configure network attributes to be retrieved from the Avaya VPN Gateway 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.**



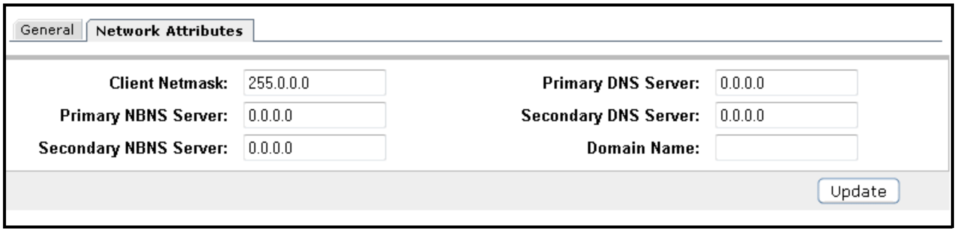
General Settings

Name: Pool_1
Status: enabled
Type: local
Proxy ARP: on
Lower IP: 10.10.100.1
Upper IP: 10.10.100.100

2. **Click Update.**

3. **Scroll down to Exclude IP Address Settings, click Add to specify IP addresses that you wish to exclude, and then click Update (optional).**

4. **Click the Network Attributes tab, and configure the desired network attributes settings in Network Attribute Settings (optional).**



Client Netmask: 255.0.0.0
Primary NBNS Server: 0.0.0.0
Secondary NBNS Server: 0.0.0.0
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0
Domain Name:

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 Step 1. 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>VPN #>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.

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

Configure RADIUS Settings

If you set the pool mechanism to `radius` (as described in the section "Create IP Pool" on page 137), you should configure the Avaya VPN Gateway to retrieve network attributes from a RADIUS server.

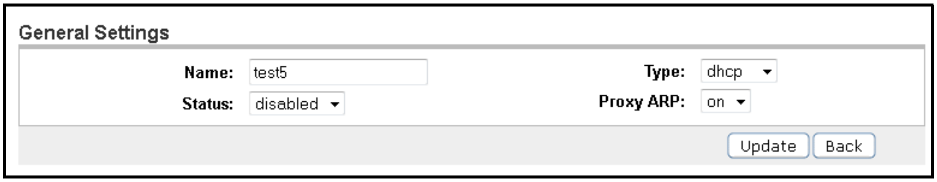
How to configure a RADIUS server is described in Chapter 9, "Authentication Methods".

To configure the Avaya VPN Gateway to retrieve network settings (including client IP address) through RADIUS attributes from an external RADIUS server, go to VPN Gateways>VPN #>Authentication>RADIUS>Network Attributes. 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 etc.

Network attributes can also be configured on the Avaya VPN Gateway 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 4 on page 140 for instructions).

Configure DHCP Settings

If you set the pool mechanism to `dhcp` (as described in the section "Create IP Pool" on page 137), you should configure the Avaya VPN Gateway to retrieve client IP address and network attributes from a DHCP server.



General Settings

Name: test5

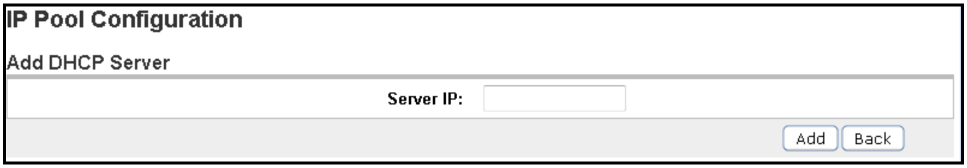
Type: dhcp

Status: disabled

Proxy ARP: on

1. **Under DHCP Servers, click Add.**

2. **Configure the external DHCP server IP address.**



IP Pool Configuration

Add DHCP Server

Server IP:

3. **Click Add.**

4. **Apply the changes.**

   Network attributes can also be configured on the Avaya VPN Gateway 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 4 on page 140 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. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on IP Pool.**

   IP Pool form appears.

5. **In the Default IP Pool list box, select an existing IP Pool as the default IP Pool.**

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

Create Host IP Pool

You can associate an IP Pool with a particular host in a clustered environment. Due to this association, the router on the private side of the cluster knows which interface is associated with each IP address allocated to the end user to send the packets back to the end user during the next hop. The interfaces supported are Net Direct (ND), Net Direct Installable Client (NDIC), Avaya VPN Client, and L2TP/IPsec.

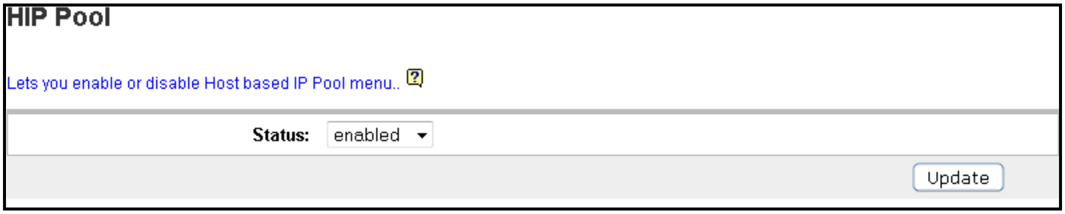
To create the Host IP Pool, perform the following:

1. **Log on to the BBI as administrator user.**
2. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to enable Host IP Pool.**

   The VPN Summary form appears.
4. **Select Host IP Pool.**

   The status form appears.



HIP Pool

Lets you enable or disable Host based IP Pool menu..

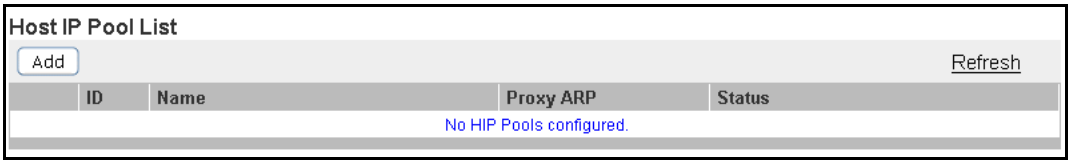
Status: enabled

5. **From the Status list, select enabled.**
6. **Click Update.**

   The VPN Summary form appears with the Host IP Address Pool option.

7. **Select the Host IP Address Pool.**

   The Host IP Pool List form appears.

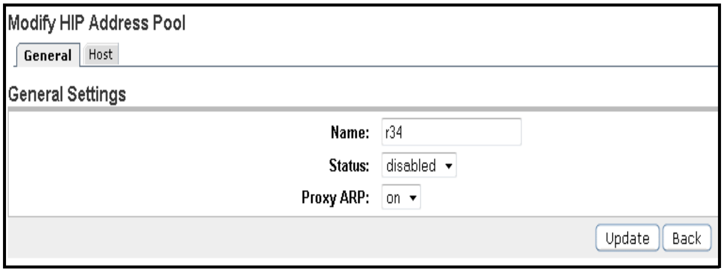


Host IP Pool List

	ID	Name	Proxy ARP	Status
No HIP Pools configured.				

8. **Click Add.**

   The Add new IP Address Pool form appears.



Modify HIP Address Pool

General Settings

Name: r34

Status: disabled

Proxy ARP: on

9. **From the HIP Pool ID list, select HIP Pool ID.**

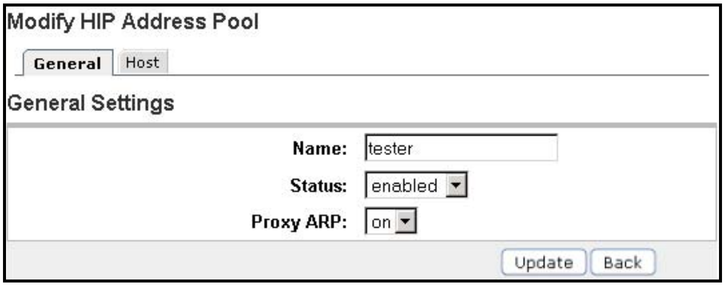
10. **In the Name field, enter the HIP Pool name.**

11. **From the Status list, select** `enabled`**.**

12. **From the Proxy ARP list, select** `on`**.**

13. **Click Update.**

    The Modify HIP Address Pool form appears.



Modify HIP Address Pool

General Settings

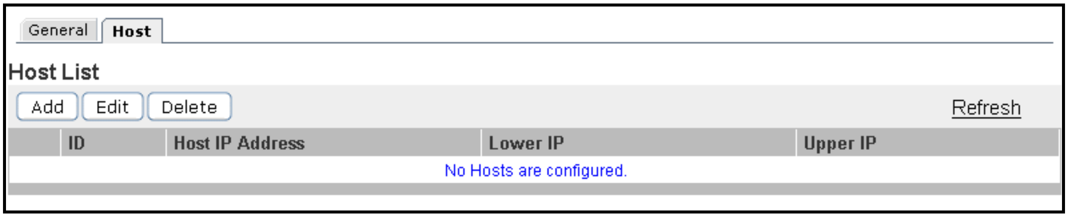
Name: tester

Status: enabled

Proxy ARP: on

14. **Click Host tab.**

    The Host List form appears.

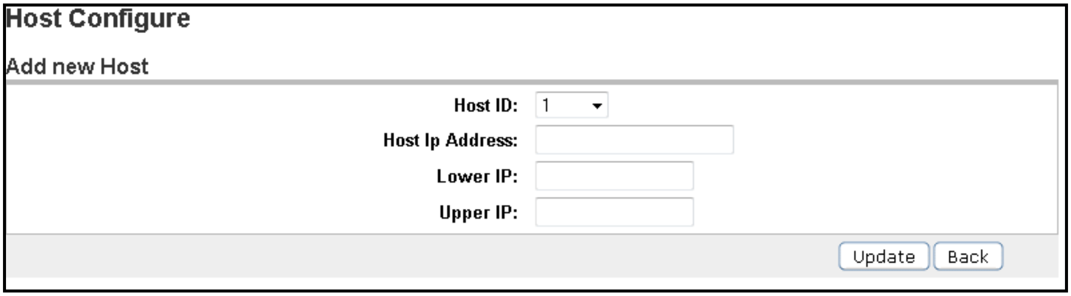


Host List

	ID	Host IP Address	Lower IP	Upper IP
No Hosts are configured.				

15. **Click Add.**

    The Add new Host form appears.



Host Configure

Add new Host

Host ID: 1
Host Ip Address:
Lower IP:
Upper IP:

16. **From the Host ID list, select Host ID.**

17. **In the Host Ip Address field, enter the Host IP address.**

18. **In the Lower IP field, enter the lower IP address of the range.**

19. **In the Upper IP field, enter the upper IP address of the range.**

20. **Click Update.**

21. **Apply changes.**

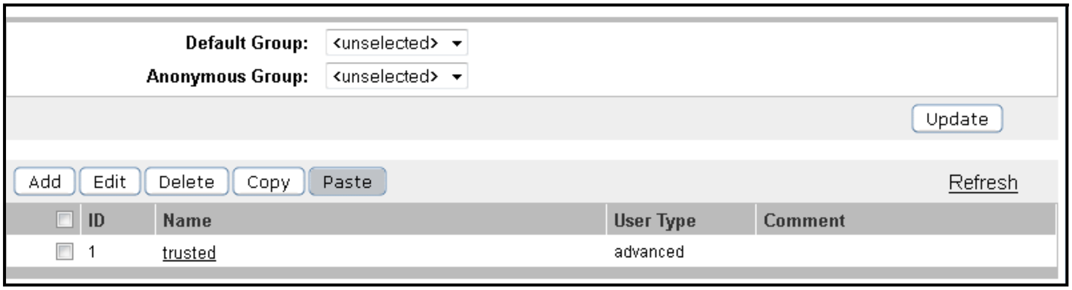
Map the IP Pool to User Group (Optional)

As mentioned on page 137, 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.

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. How to create a default IP Pool is described in the next section.

Follow these steps to map an IP Pool to a user group:

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on Groups settings.**
5. **Select the check box next to the group to which you want to map an IP Pool.**



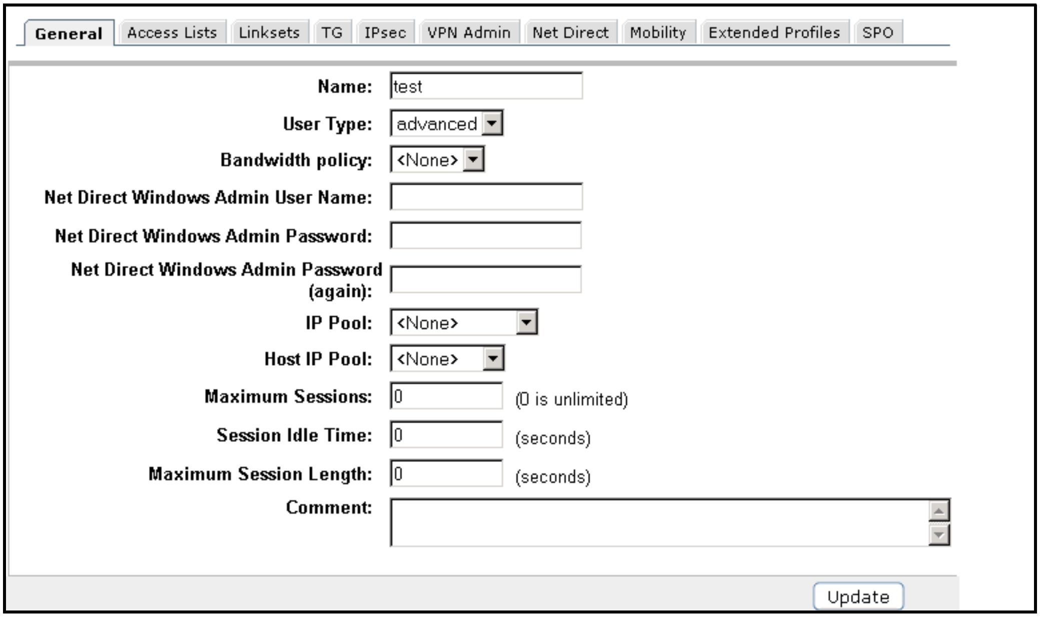
Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

6. **Click Edit.**

7. **In the IP Pool list, select the IP Pool that you want to map to the current group.**



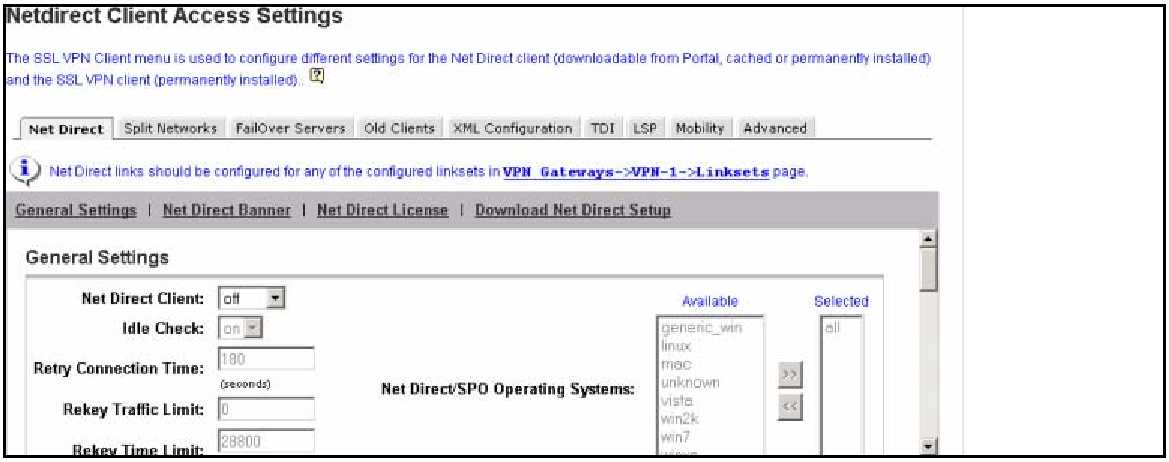
Name:	test
User Type:	advanced
Bandwidth policy:	<None>
Net Direct Windows Admin User Name:	
Net Direct Windows Admin Password:	
Net Direct Windows Admin Password (again):	
IP Pool:	<None>
Host IP Pool:	<None>
Maximum Sessions:	0 (0 is unlimited)
Session Idle Time:	0 (seconds)
Maximum Session Length:	0 (seconds)
Comment:	

8. **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. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on VPN Client settings.**
5. **Click Net Direct.**



Netdirect Client Access Settings

The SSL VPN Client menu is used to configure different settings for the Net Direct client (downloadable from Portal, cached or permanently installed) and the SSL VPN client (permanently installed).

Net Direct links should be configured for any of the configured linksets in VPN Gateways->VPN-1->Linksets page.

General Settings | Net Direct Banner | Net Direct License | Download Net Direct Setup

General Settings

Net Direct Client: off
Idle Check: on
Retry Connection Time: 180 (seconds)
Rekey Traffic Limit: 0
Rekey Time Limit: 28800

Net Direct/SPO Operating Systems:
Available: generic_win, linux, mac, unknown, vista, win2k, win7
Selected: all

6. **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.
   - `off`: Net Direct client access is disabled.
   - `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 #>Group Settings>Groups>General** form, display the desired group and select `on` in the Net Direct client list box.

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 Step 7 to Step 15):

7. **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.

8. **In the Retry Connection Time field, enter the desired value.**

   This setup sets the maximum timeout for reconnection if the Net Direct connectivity to the server is lost. Reconnection helps restore the Net Direct session without user intervention.

   The default value is 180 seconds (3 minutes). If you set it to 0, the service will be disabled. The valid range is 60-3600 seconds, that is, 1minute to 60 minutes.

   The field is editable only if Net Direct Client is on.

9. **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 Avaya 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.

10. **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 Avaya 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.

11. **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 uses configured ports for sending encrypted UDP packets to the Avaya VPN Gateway. If this fails (due to for example firewalls between the client and the Avaya 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.

To disable the UDP ports, the port range 0-1 needs to be specified.

12. **In the MSS Clamping list box, verify that the desired setting is selected.**

    - `on`: The Avaya VPN Gateway 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 Avaya VPN Gateway 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 are subject to fragmentation. This results in a slower connection.

13. **In the Caching list box, specify whether or not caching of Net Direct components on the client machine should be allowed (only for Net Direct on Windows).**

    - `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.

14. **From the Portal Bind list, select on.**

    The default value is on. The browser closes the Net Direct when the user logs off the Portal or moves away from the Portal.

NOTE – The portal bind off setting is not supported on Linux platforms. On this platform, the Net Direct client behaves as if the portal bind setting is on. Portalbind is not supported on the Macintosh platform.

NOTE – If portal bind is off, the EACA mode must be disabled, or, if enabled, configure EACA as runonce mode.

15. **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 Avaya 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.
- `generic_win`: Net Direct clients running on any other Windows version are allowed to connect.
- `linux`: Net Direct clients running on Linux are allowed to connect.
- `mac`: Net Direct clients running on Mac OS X are allowed to connect.
- `unknown`: Net Direct clients running on an OS that cannot be identified (for example new OS
  versions) are allowed to connect.
- `win2k`: Net Direct clients running on Windows 2000 are allowed to connect.
- `winxp`: Net Direct clients running on Windows XP are allowed to connect.

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

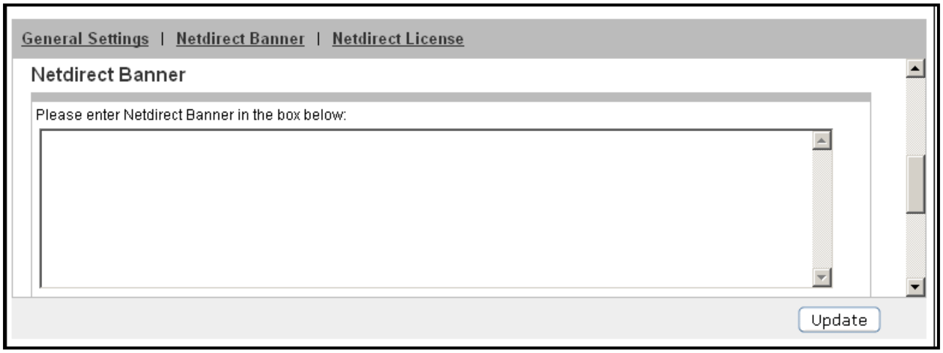
Banner Text

To configure a banner message to be displayed to the user when Net Direct is successfully downloaded and/or installed, proceed as follows:

1. **Scroll down to the Net Direct Banner text box.**

   Or click Net Direct Banner in the gray area in the Net Direct Client Access Settings form.

2. **In the text box, enter or paste the desired banner text.**



General Settings | Netdirect Banner | Netdirect License
Netdirect Banner
Please enter Netdirect Banner in the box below:
Update

3. **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 163.

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. **Scroll down to the Net Direct License text box.**

   Or click Net Direct License in the gray area in the Net Direct Client Access Settings form.

2. **In the text box, enter or paste the desired license text.**

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

   Also see the section "Net Direct from a User Perspective" on page 163.

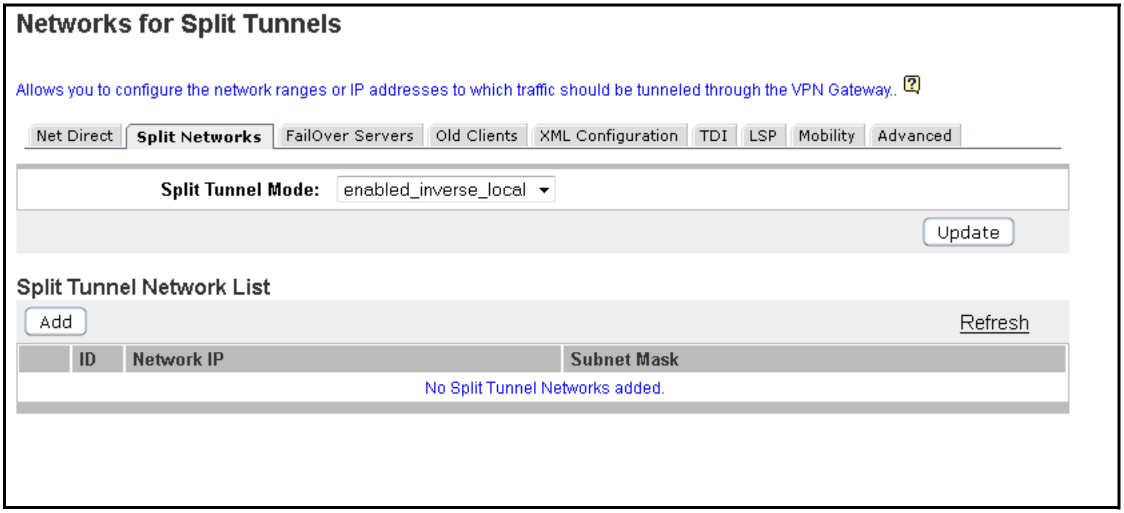
   The license text window is not displayed for the installed Net Direct client.

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 Avaya VPN Gateway or directly to the Internet.

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on VPN Client settings.**
5. **Select Split Networks.**

   The Networks for Split Tunnels form is displayed.



Networks for Split Tunnels

Allows you to configure the network ranges or IP addresses to which traffic should be tunneled through the VPN Gateway..

Split Tunnel Mode: enabled_inverse_local

Split Tunnel Network List

	ID	Network IP	Subnet Mask
		No Split Tunnel Networks added.	

6. **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 Avaya VPN Gateway.
   - `enabled`. Tunnels traffic to *specified networks* (see the next step) to the Avaya 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 Avaya VPN Gateway.

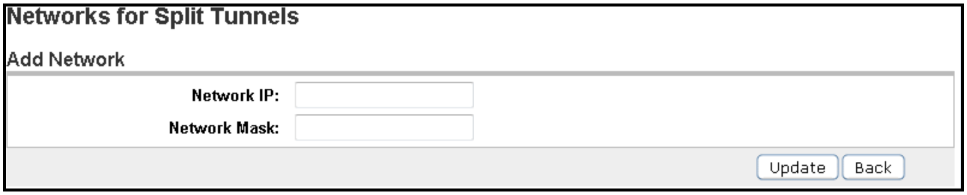
- `enabled_inverse_local`. Does *not* tunnel traffic to directly connected networks or to specified networks (see the next step). This will for example allow the remote user to print locally, even while tunneled to the Avaya VPN Gateway. All other network traffic is tunneled through the Net Direct client to the Avaya VPN Gateway. This is the default setting.

NOTE – The Mac OS X modes `enabled_inverse` and `disabled` modes do not tunnel the local net. The `enabled_inverse` mode is not supported on the Linux operating system. 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` mode will be used as fallback.

7. **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).

8. **Under Split Tunnel Network List, click Add.**



Networks for Split Tunnels

Add Network

Network IP:

Network Mask:

9. **In the Network IP field, enter the network IP address to be tunneled.**
10. **In the Network Mask field, enter the desired network mask.**
11. **Click Update.**
12. **Add another network in the same way, by repeating Step 8 to Step 11.**
13. **Apply the changes.**

Configure Net Direct Link

1. **Log in to the BBI as administrator user.**

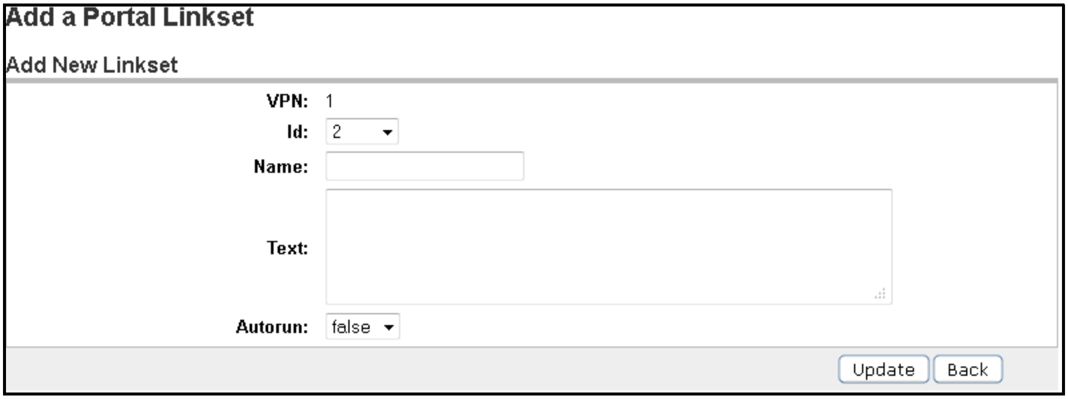
2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Select Linkset settings.**

5. **Click Add.**

   The Portal Linkset Configuration form is displayed.



Add a Portal Linkset

Add New Linkset

VPN:	1
Id:	2
Name:	
Text:	
Autorun:	false

6. **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.

7. **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, e.g. <b>heading</b> to create a boldface heading.

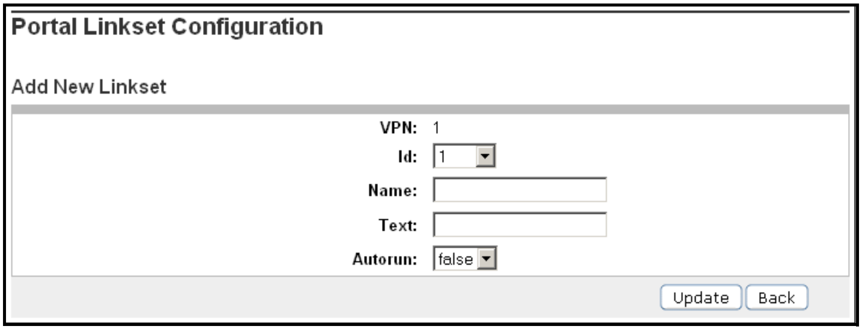
8. **In the Autorun list box (optional), make the desired selection.**

   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.

9. **Click Update.**

10. **Click Add.**

The Portal Linkset Configuration form is displayed.



Portal Linkset Configuration

Add New Linkset

VPN: 1

Id: 1

Name:

Text:

Autorun: false

11. **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.

12. **Click Update.**

13. **In the System tree view, select VPN Gateway.**

14. **Select Linksets.**

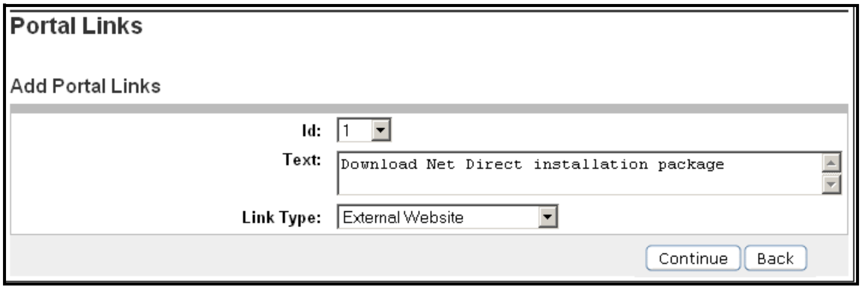
15. **Select the name of portal linkset and then click on Portal Links tab.**

16. **Click Add.**

The Add Portal Links form is displayed.

17. **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`.**

18. **In the Link Type list box, select the External Website link type.**



Portal Links

Add Portal Links

Id: 1

Text: Download Net Direct installation package

Link Type: External Website

19. **Click Continue.**

The form is expanded.

20. **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. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Select Group settings.**

   The Groups form is displayed.
5. **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 Chapter 8, "Groups, Access Rules and Profiles". You can also map the linkset to an existing group. In this case, skip this step and continue with the next step.
6. **Expand Groups and select Linksets.**
7. **Verify that the correct VPN and group id/name are displayed in the VPN Number and Group list boxes, respectively.**
8. **In the Portal Linksets list box, select the linkset we have just created (that is, netdirect) and click Add.**
9. **Apply the changes.**

Configure Windows 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 Windows administrator user name and password on the Avaya VPN Gateway. The credentials are stored on group level.

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 Windows 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. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Select Group settings.**
5. **Verify that the desired VPN and group id/name are displayed in the VPN Number and Group list boxes, respectively.**
6. **In the Net Direct Admin Windows User Name field, enter the Windows administrator user name.**
7. **In the Net Direct Windows Admin Password fields, enter the Windows administrator password.**
8. **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 Step 13 in the section "Enable Net Direct" on page 148.

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. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Select Linksets settings.**
5. **Click Add.**

   The Portal Linkset Configuration form is displayed.
6. **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.
7. **Click Update.**
8. **In the System tree view, select VPN Gateway.**
9. **Select Linksets.**
10. **Select the name of portal linkset and then click on Portal Links tab.**
11. **Click Add.**

    The Add Portal Links form is displayed.
12. **In the Text field, enter the clickable link text to be displayed on the Portal’s Home tab, e.g. `Download Net Direct installation package`.**
13. **In the Link Type list box, select the External Website link type.**
14. **Click Continue.**

    The form is expanded.
15. **Under External Link Settings, in the Protocol list box, select `https`.**
16. **In the Host field, enter the Portal’s host name or IP address. For example, vpn.example.com.**
17. **In the Path field, enter /nortel_cacheable/NetDirect_Setup.zip.**
18. **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. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Select Groups settings.**
5. **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 Chapter 8, "Groups, Access Rules and Profiles".

   You can also map the linkset to an existing group. In this case, skip this step and continue with the next step.

6. **Click on Group Name and select Linksets.**
7. **Verify that the correct group id/name is displayed in the Group list box.**
8. **In the Portal Linksets list box, select the linkset we have just created (that is, `installed_ND`) and click Add.**
9. **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 Chapter 6, “The Portal from an End-User Perspective”.

1. **Follow the instructions for enabling Net Direct client access previously in this chapter.**

2. **Log in to the BBI as administrator user.**

3. **Click on Config tab.**

4. **Click on the VPN gateway name.**

5. **Select Portal settings and click on Full Access List tab.**

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

Net Direct from a User Perspective

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 156). Consider the following 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 164) 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 in the section “Installed Version (Windows)” on page 164 beginning with Step 8.

   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 Windows administrator password is stored in the CLI for the group in which the user is member (see “Configure Windows Administrator User Name/Password” on page 158), a progress bar is displayed while the Net Direct client is being downloaded.

   If the user does not have administrator privileges on the PC, a dialog box displays the question “Do you want to enter Administrator details? Press Yes, No to Exit.”

4. **Click Yes if you have access to the Windows administrator user name and password for the PC.**

   If you click No, the process of downloading Net Direct will be cancelled.

5. **Enter the Windows 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 153), a License Agreement dialog box displays.

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. If you click Cancel, Net Direct exits.

   NOTE – The Net Direct client will not be started if the installable Avaya 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 153), a welcome banner displays.

7. **Click OK.**

   When the Net Direct client is fully installed and has connected to the VPN server (that is, the Avaya VPN Gateway), this is confirmed with an icon being displayed on the system tray.

   By right-clicking the system tray icon and selecting **Status**, you can view connection details.

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 160). Consider the following instructions as directed to the user.

1. **Log in to the Portal.**

2. **Click the download link.**

A file download window appears.

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 Net Direct Client icon on your desktop or select 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, e.g. 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 configured, the banner message window (see "License Text" on page 153) displays.

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**, you can view connection details.

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 Avaya VPN Gateway, 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.

Preconfigure and customize Net Direct Client

The preconfiguration and customization of the Net Direct distribution can be done using the NetDirect.xml file. This file comes along with the distribution file (NetDirect_Setup.zip). The NetDirect.xml file specifies the list of connection profiles and this can be imported into the NDIC, which will update the list of connection profiles along with this new values.

You can specify the following details in the connection profile:

- Connection Name
- Server Address
- Port
- Authentication Service
- UserName
- Connection Description

A sample NetDirect.xml is as follows:

```
<?xml version="1.0" encoding="utf-8" ?>
 <configuration name="NetDirect Config file" version="0.1">
  <servers>
   <item>
   <name>My connection</name>
   <address>1.1.1.1</address>
   <port>443</port>
    <authservice>default</authservice>
    <username>user1</username>
    <description>Test Connection Profile</description>
    </item>
    </servers>
    </configuration>
```

Create a Net Direct XML

Follow these steps to create a Net Direct XML file:

1. **Place the connection profile details between the <servers> and </servers> tags.**
2. **Each connection profile will starts with <item> tag and ends with </item> tag.**

   Therefore, you can add as many connection profiles by including as many <item>/</item> tags.

3. **Each entry in a connection profile can be specified as follows:**
   - Connection Name: Include your text between <name> and </name> tags.
   - Server Address : Include your text between <address>and </address> tags.
   - Port: Include your text between <port>and </port> tags.
   - Authentication Service: Include your text between <authservice> and </authservice> tags.

- □ UserName: Include your text between <username> and </username> tags.
- □ Connection Description: Include your text between <description> and </description> tags.

Import Net Direct XML

Once the Net Direct.xml is updated with connection profile details, you can import it to NDIC using the following methods:

Method 1:

1. **Launch NDIC.**
2. **Click File->Import.**

   Display a file selection dialog box is displayed.
3. **Select the updated NetDirect.xml file and click "OK".**

Method 2:

To use this method, stop the NDIC if running.

1. **Go to the Installation path of NDIC.**
2. **Place the updated NetDirect.xml file in this path. If it already exists, Overwrite it.**

NOTE – Overwriting the existing file results in loss of all the previously saved profile details in that NDIC.

3. **Launch the application.**

   The connection profile list is updated.

Method 3:

1. **The release package contains an empty NetDirect.xml file.**
2. **Update the necessary connection profile details to send the profiles to the client machine.**
3. **During installation, this file is placed in the installation folder of the NDIC and the profiles will be updated.**

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 156). Consider the following instructions as directed to the user.

1. **Start Safari and log in to the Portal.**

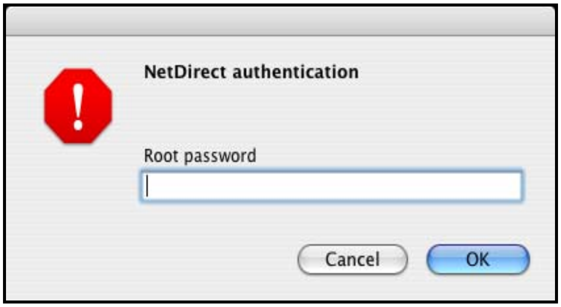
2. **Click the Net Direct link.**

   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.



NetDirect authentication

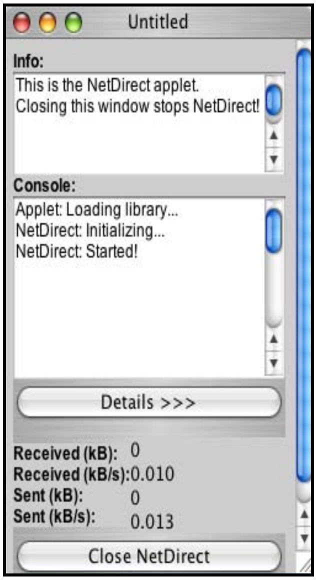
Root password

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 Avaya VPN Gateway), this is confirmed in the Java applet window.



Info:

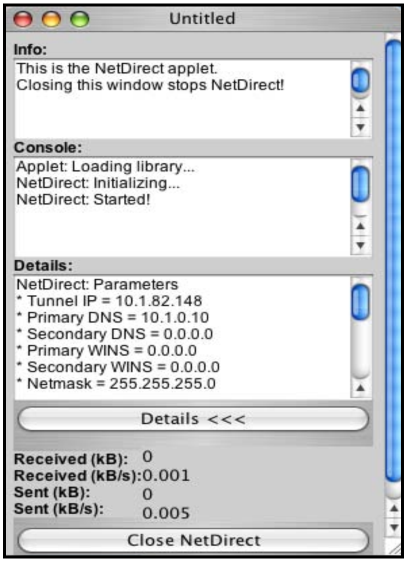
This is the NetDirect applet.
Closing this window stops NetDirect!

Console:

```
Applet: Loading library...
NetDirect: Initializing...
NetDirect: Started!
```

Received (kB): 0
Received (kB/s):0.010
Sent (kB): 0
Sent (kB/s): 0.013

Click the Details button to display connection details:



Info:

This is the NetDirect applet.
Closing this window stops NetDirect!

Console:

```
Applet: Loading library...
NetDirect: Initializing...
NetDirect: Started!
```

Details:

```
NetDirect: Parameters
* Tunnel IP = 10.1.82.148
* Primary DNS = 10.1.0.10
* Secondary DNS = 0.0.0.0
* Primary WINS = 0.0.0.0
* Secondary WINS = 0.0.0.0
* Netmask = 255.255.255.0
```

Received (kB): 0
Received (kB/s):0.001
Sent (kB): 0
Sent (kB/s): 0.005

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.

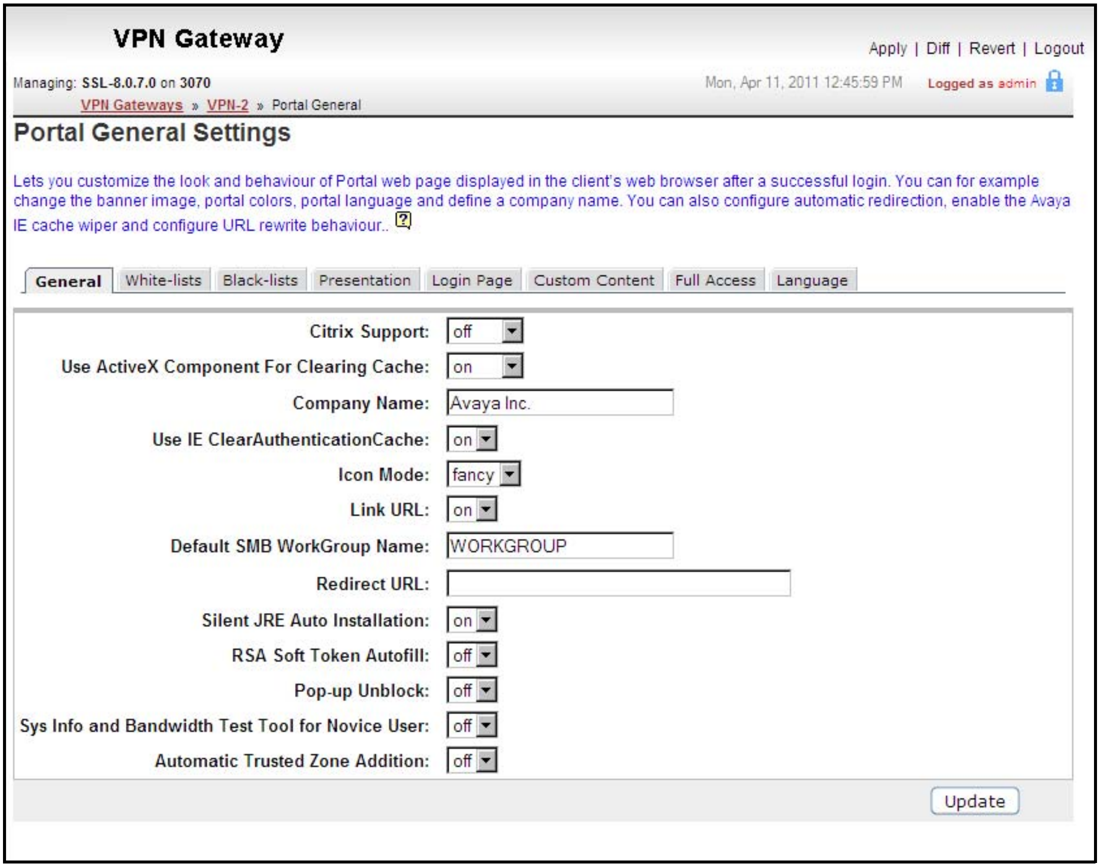
   If errors should occur, the `NetDirectError.log` file is created under `/tmp` on the client machine. This is the same path as for Linux.

Start Net Direct Outside Portal

The Avaya VPN Gateway can be configured to redirect the remote user to another web page (for example corporate Portal), thus by-passing the Avaya VPN Gateway Portal altogether. This section describes the steps involved to be able to start the Net Direct client from the internal page.

For automatic login to the internal page, see the next section.

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Select Portal settings and click on General tab in Portal General Settings screen.**


VPN Gateway
Apply | Diff | Revert | Logout
Managing: SSL-8.0.7.0 on 3070
Mon, Apr 11, 2011 12:45:59 PM
Logged as admin
VPN Gateways » VPN-2 » Portal General
General
White-lists
Black-lists
Presentation
Login Page
Custom Content
Full Access
Language
Update

Portal General Settings

Lets you customize the look and behaviour of Portal web page displayed in the client's web browser after a successful login. You can for example change the banner image, portal colors, portal language and define a company name. You can also configure automatic redirection, enable the Avaya IE cache wiper and configure URL rewrite behaviour..

Citrix Support: off
Use ActiveX Component For Clearing Cache: on
Company Name: Avaya Inc.
Use IE ClearAuthenticationCache: on
Icon Mode: fancy
Link URL: on
Default SMB WorkGroup Name: WORKGROUP
Redirect URL:
Silent JRE Auto Installation: on
RSA Soft Token Autofill: off
Pop-up Unblock: off
Sys Info and Bandwidth Test Tool for Novice User: off
Automatic Trusted Zone Addition: off

5. **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`**

6. **Click Update.**

7. **Apply the changes.**

8. **On the web server to which the user should be redirected, insert the following script (see next page):**

```
<html>
<head>
<title></title>
<script language="javascript">
function enable1()
{
OcxRet =
NetDirectOCX.StartDownLoad ('/nortel_cacheable/NetClient.zip',
'443', '', '', document.MyForm.serverip.value,
document.MyForm.uname.value,
document.MyForm.uid.value,'','','');
}
</script>
</head>
<body>
<OBJECT id=NetDirectOCX style="LEFT: 0px; TOP: 0px"
codeBase="https://YourAVGAddress/nortel_cacheable/NetDirect.cab#VERSION=6,0,1"
height=0 width=0
classid=clsid:7fa319fb-ffb9-4089-87eb-63179244e6e6>
<PARAM NAME="_Version" VALUE="65536"><PARAM NAME="_ExtentX"
VALUE="26">
<PARAM NAME="_ExtentY" VALUE="26"><PARAM NAME="_StockProps"
VALUE="0"></OBJECT>
<form id="MyForm" name="MyForm">
<center><font size="+1"
color=blue><b><i>Welcome to the Avaya VPN Gateway</i><p>
Login<p>
Server Alias
<INPUT style="LEFT: 78px; TOP: 2px" type=test
name=serverip><p>
UserName
<INPUT name=uname><p>
Password
<INPUT type=password name=uid><p>
<INPUT type="button"
name="enable" value="Enable NetDirect"
onclick="javascript:enable1();">
<p>
</b></font></center><br></form>
</body>
</html>
```

Make sure that the correct version of the Net Direct client is specified. In the OBJECT tag in the preceding example, version `6.0.1` will be downloaded from the Avaya VPN Gateway.

Note that the sample html code on the previous page is not production code. Error handling adapted to your application should also be added.

Also note that newlines inserted into the script may damage the script.

Start Net Direct Outside Portal with Auto-Login

This example shows how to automatically log in the remote user to the internal site.

1. **In the Redirect URL field, enter an URL like the following:**

   Example:
   `http://<var:portal>/http/InternalWebServer/NetDirect.asp?portal=<var:portal>&user=<var:user>&password=<var:password>`

2. **On the web server to which the user should be redirected, insert the following script:**

```
<%@ Language=VBScript %>
<HTML>
<HEAD>
<TITLE>NetDirect</TITLE>
</HEAD>
<BODY>
<OBJECT id=NetDirectOCX style="LEFT: 0px; TOP: 0px"
codeBase="https://YourAVGAddress/nortel_cacheable/NetDirect.cab#VERSION=6,0,1"
height=0 width=0
classid=clsid:7fa319fb-ffb9-4089-87eb-63179244e6e6><PARAM
NAME="_Version" VALUE="65536"><PARAM NAME="_ExtentX"
VALUE="26"><PARAM NAME="_ExtentY" VALUE="26"><PARAM
NAME="_StockProps" VALUE="0"></OBJECT>
Hello <%= Request.QueryString("user") %> : <%=
Request.QueryString("password")%>.
You want to access <%= Request.QueryString("portal") %>!
<%
If Request.QueryString("UserStatus") = "New" Then
Response.Write "If you have any problems with the site call the helpdesk!"
End If
Dim portal
portal = Request.QueryString("portal")
Response.Write "<SCRIPT LANGUAGE=JavaScript>
NetDirectOCX.StartDownLoad('/nortel_cacheable/
NetClient.zip', '443', '', '', '" & Request.QueryString
("portal") & "', '" & Request.QueryString
("user") & "', '" & Request.QueryString("password") & "', '', '', '');</SCRIPT>"
%>
</BODY>
</HTML>
```

Make sure that the correct version of the Net Direct client is specified. In the OBJECT tag in the preceding example, version `6.0.1` will be downloaded from the Avaya VPN Gateway.

Note that the sample html code is not production code. Error handling adapted to your application should also be added.

Also note that newlines inserted into the script may damage the script.

CHAPTER 8
Groups, Access Rules and Profiles

This chapter describes the authorization part of the AAA system, i.e. 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 Avaya VPN Gateway. If local database authentication is used, the user's user name and password should be configured in the Avaya 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 Chapter 9, "Authentication Methods".

Group Parameters

All the group's members will share the limitations and capabilities that you assign to the group. The most important parameters form the group's access rules, that is, the rules that control which hosts and subnets the group member should be authorized to (or *not* authorized to).

The following parameters can be configured for a group:

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

Linksets

Each user group can be provided 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.

For instructions on how to create linksets and links, see Chapter 11, "Group Links".

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, i.e. also the Advanced tab.
- Normal.

For a description of the Portal tabs, see Chapter 6, "The Portal from an End-User Perspective".

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.

The file extension definition can also be used as an access rule. File extension definition identifies the specific filename extensions that can be made accessible to authorized user.

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, expand **VPN Gateway>VPN# >Groups**. In the **Default Group** list box, select the group to be used as the default group.

Extended Profiles

Extended profiles can be created 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 208.

Secure Portable Office

The Secure Portable Office (SPO) client provides remote access for Avaya Applications. For instructions on how to configure SPO, see Chapter 13, "Secure Portable Office Client".

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 (i.e. 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 Gateway>VPN# > General settings**. It can also be configured on group level (see section "Group Configuration" on page 196) 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 Gateway>VPN# > General settings**. It can also be configured on group level (see "Group Configuration" on page 196) 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 VPN Client connections, an IP Pool has to be configured, under **VPN Gateway>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 Chapter 7, "Net Direct" and Chapter 21, "Transparent Mode".

Avaya Endpoint Access Control Agent Rules

By mapping a Avaya Endpoint Access Control Agent SRS rule to a group, the all group members will be subject to a Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent, along with configuration instructions, see Chapter 15, "Configure Avaya Endpoint Access Control Agent".

IPsec Tunnel Access

For a group member to be able to log in to the VPN with the Avaya 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 VPN Client, along with configuration instructions, see Chapter 21, "Transparent Mode".

IE Cache Wiper

Whether or not remote users should be able to install the 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 IE Cache Wiper). The 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 session are 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 Avaya VPN Gateway 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 Chapter 7, “Net Direct”.

Windows Administrator User Name/Password

You can also configure a common Windows 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 Avaya 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.

Following is a list of parameters and how they are treated when a user belongs to several groups:

- ***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***. 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.

L2TP

The group must be mapped to an existing user tunnel profile for a group member to log in to the VPN with the Layer 2 Tunneling Protocol (L2TP). For more information about L2TP access, see “Layer 2 Tunneling Protocol” on page 559.

NAP

Network Access Protection (NAP) provides system health validation access to the private networks. To limit the access of network client until the health policy requirements are met, enable TG and configure NAP. For more information about configuring NAP, see “Network Access Protection” on page 593.

AAA Configuration Order

From top to bottom, the 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 Avaya VPN Gateway. If local database authentication is used, both users and groups should be configured on the Avaya 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 Avaya VPN Gateway's local database or client certificate authentication. The steps are described in Chapter 9, "Authentication Methods".
- **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 Chapter 11, "Group Links".
- **Configure users**. If local database authentication is used, the user should be configured on the Avaya VPN Gateway. This is also where to map the user to one or several previously defined groups. The steps are described in Chapter 9, "Authentication Methods".

Extended Profiles

If extended profiles should be applied to groups, a couple of more steps are involved. See the section "Working with Extended Profiles" on page 208 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 in the section "Group Configuration" on page 196.

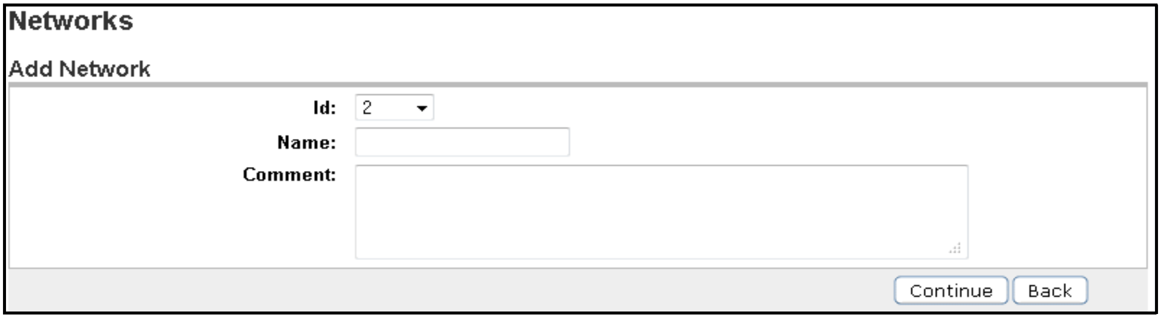
Create Network Definitions

Access to Outlook Web Access Server

This example describes how to create a network definition identifying an Outlook Web Access server on the intranet.

1. **Log on to the BBI as system administrator.**
2. **Click on Config Tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Under Settings, select Authorization.**
5. **Click Add.**

   The Add Network form is displayed.



Networks

Add Network

Id: 2

Name:

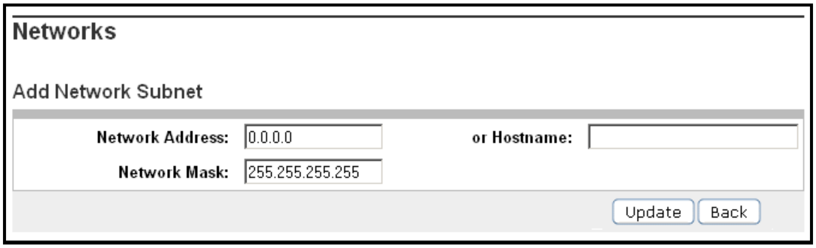
Comment:

6. **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.

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

The Add Network Subnet form is displayed.



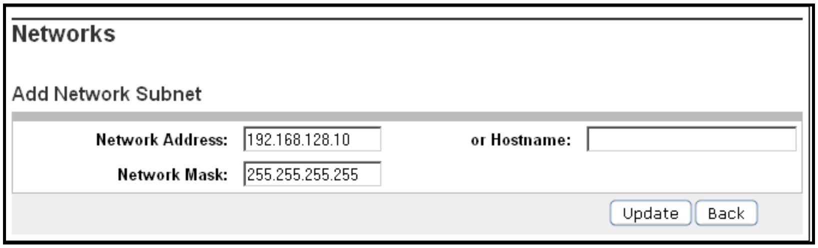
Networks

Add Network Subnet

Network Address:	0.0.0.0	or Hostname:	
Network Mask:	255.255.255.255		

8. **In the Network Address and Network Mask 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.



Networks

Add Network Subnet

Network Address:	192.168.128.10	or Hostname:	
Network Mask:	255.255.255.255		

9. **Click Update.**

The subnet is added to the network list.

10. **Apply the changes.**

We will use this network definition in an access rule in the example in the section “Configure Access Rule 1” on page 198.

Access to Intranet Web Server

This example describes how to create a network definition identifying a web server on the intranet. The steps are the same as in the previous example, except for the network name and host IP address.

1. **Log on to the BBI as system administrator.**

2. **Click on Config Tab.**

3. **In the system tree view, select VPN Gateways.**

4. **Under Settings, select Authorization.**

5. **Click Add.**

   The Add Network form is displayed.

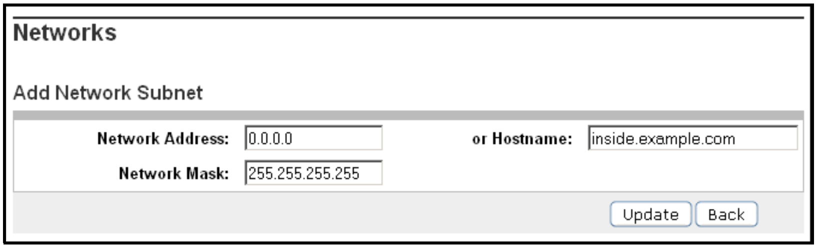
6. **In the Name field, enter a network name and click Continue.**

   In this example we will create a network definition called `webserver`. The form is expanded to show the Network Subnets list.

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

   The Add Network Subnet form is displayed.

8. **In the Network Address and Network Mask fields, enter a subnet (and netmask) identifying the intranet web server.**
   OR
   Enter the web server's host name in the Hostname field.



Networks

Add Network Subnet

Network Address: 0.0.0.0

or Hostname: inside.example.com

Network Mask: 255.255.255.255

9. **Click Add.**

   The subnet is added to the subnet list.

10. **Apply the changes.**

Access to Intranet File Server

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

1. **Log on to the BBI as system administrator.**
2. **Click on Config Tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Under Settings, select Authorization.**
5. **Click Add.**

   The Add Network form is displayed.

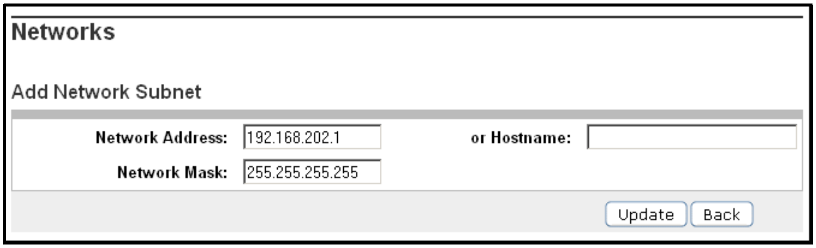
6. **In the Name field, enter a network name and click Continue.**

   In this example we will create a network definition called `fileserver`. The form is expanded to show the Network Subnets list.

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

   The Add Network Subnet form is displayed.

8. **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.



Networks

Add Network Subnet

Network Address:	192.168.202.1	or Hostname:	
Network Mask:	255.255.255.255		

9. **Click Update.**

   The subnet is added to the subnet list.

10. **Apply the changes.**
11. **In the System tree view, under VPN Gateways>VPN #>Group Settings, select Networks to view the network definitions we have just created.**

Access Allowed to Specific Subnet

This example describes how to create a network definition identifying a specific subdomain in a company's intranet to which the group members should be authorized. The subdomain is called `sales.example.com`.

1. **Log on to the BBI as system administrator.**
2. **Click on Config Tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Under Settings, select Authorization.**
5. **Click Add.**

   The Add Network form is displayed.

6. **In the Name field, enter a network name and click Continue.**

   In this example we will create a network definition called `sales`. The form is expanded to show the Network Subnets list.

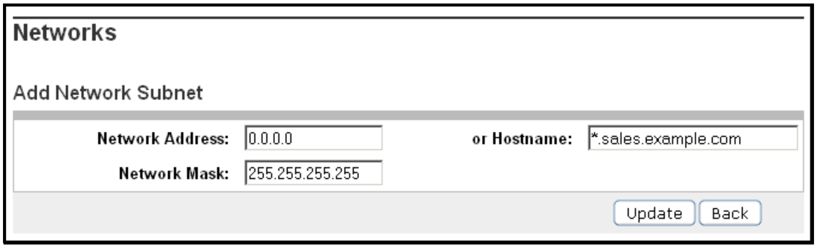
7. **Under Network Subnets, click Add.**

   The Add Network Subnet form is displayed.

8. **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.



Networks

Add Network Subnet

Network Address: 0.0.0.0   or Hostname: *.sales.example.com

Network Mask: 255.255.255.255

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

NOTE – You can create a network definition consisting of *several* subnet definitions.

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 to the BBI as system administrator.**
2. **Click on Config Tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Under Settings, select Authorization.**
5. **Click Add.**

   The Add Network form is displayed.

6. **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.

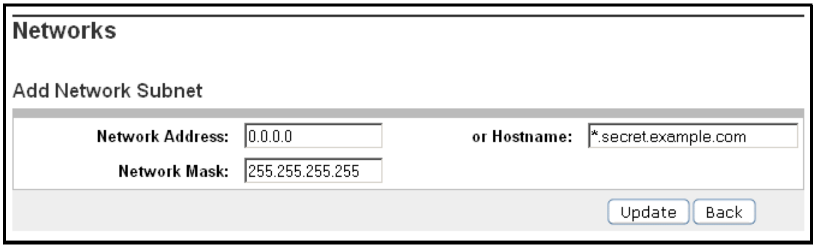
7. **Under Network Subnets, click Add.**

   The Add Network Subnets form is displayed.

8. **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.



Networks

Add Network Subnet

Network Address: 0.0.0.0

or Hostname: *.secret.example.com

Network Mask: 255.255.255.255

9. **Click Update.**

10. **Apply the changes.**

    We will later reference these network definitions in different access rules in the group configuration examples in the section “Group Configuration” on page 196.

Create Service Definitions

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

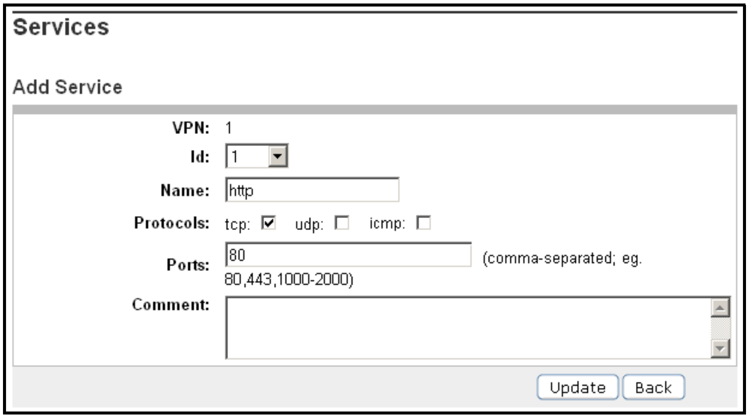
Access to HTTP Protocol

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

1. **Logon to the BBI as administrator.**
2. **Click on Config tab.**
3. **Select VPN Gateways.**

   The VPN Gateways form is displayed.
4. **Select the name of the VPN Gateway.**
5. **Under settings, select Authorization**
6. **Select Services and click Add.**

   The Add Service form is displayed.



Services

Add Service

VPN: 1

Id: 1

Name: http

Protocols: tcp: ☑ udp: ☐ icmp: ☐

Ports: 80 (comma-separated; eg. 80,443,1000-2000)

Comment:

7. **In the Name field, enter a name for the service.**

   In this example we will create a service definition called http.

8. **Check allowed protocols.**

9. **Specify allowed port numbers.**

   For HTTP, enter 80.

10. **Click Update.**

11. **Apply the changes.**

    Reference is made to this service definition in an access rule in the group configuration examples in the section "Group Configuration" on page 196.

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. **Logon to the BBI as administrator.**

2. **Click on Config tab.**

3. **Select VPN Gateways.**

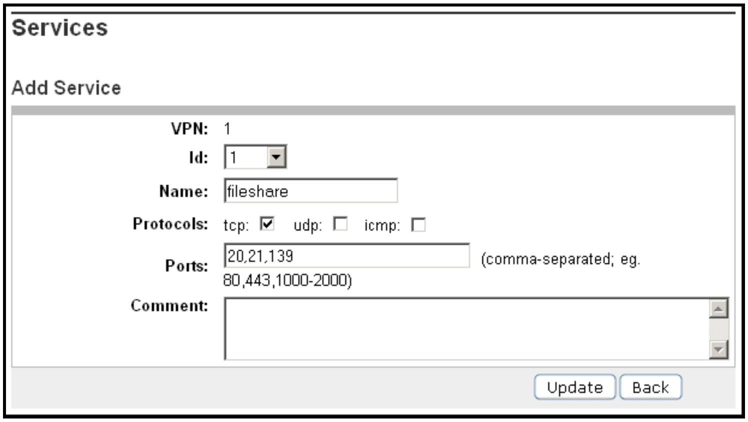
   The VPN Gateways form is displayed.

4. **Select the name of the VPN Gateway.**

5. **Under settings, select Authorization.**

6. **Select Services and click Add.**

The Add Service form is displayed.



Services

Add Service

VPN:	1
Id:	1
Name:	fileshare
Protocols:	tcp: ☑ udp: □ icmp: □
Ports:	20,21,139 (comma-separated; eg. 80,443,1000-2000)
Comment:	

7. **In the Name field, enter a name for the service.**

   In this example we will create a service definition called `fileshare`.

8. **Check allowed protocols.**

9. **Specify allowed port numbers.**

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

10. **Click Update.**

11. **Apply the changes.**

    Reference is made to this service definition in an access rule in the group configuration examples in the section "Group Configuration" on page 196.

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. This Appspec definition in an access rule is referenced later in this document, and the `web-server` network definition created in the example on page 186 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:

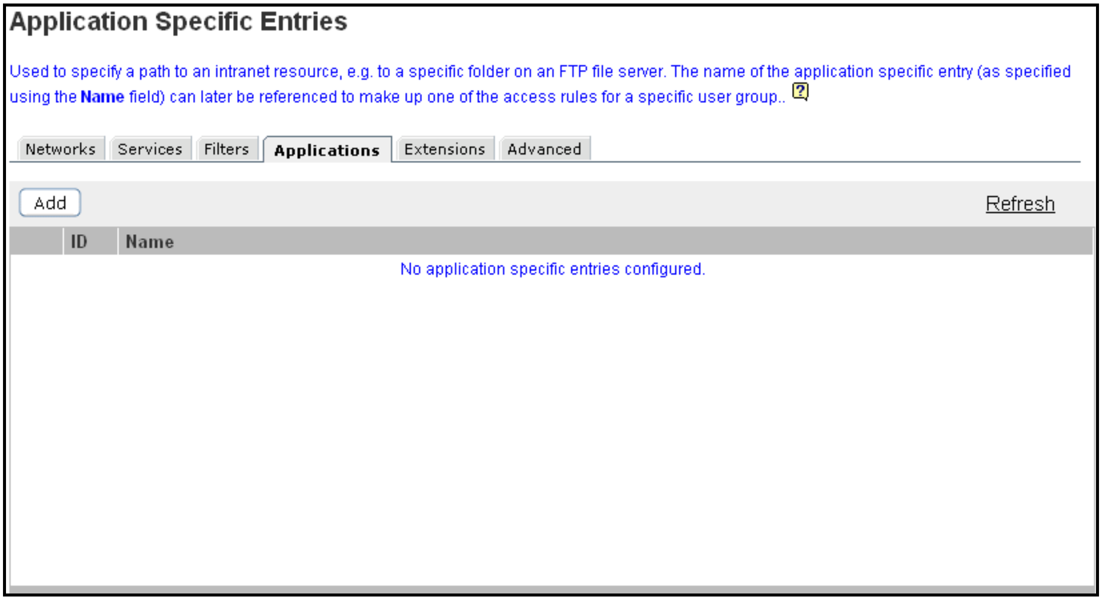
- For SMB, write the path as /WORKGROUP/FILESHARE/FILE PATH, e.g. **`/AVAYA/homes/public`**. This will give access to the `public` directory in the `homes` share in the `AVAYA` workgroup/domain.
- For FTP, write the path as ABSOLUTE FILE PATH, e.g. **`/home/share/public/`**. This will give access to 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, e.g. **`/intranet`**. This will give access to the `/intranet` path on the web server.

1. **Logon to the BBI as administrator.**
2. **Click on Config tab.**
3. **Select VPN Gateways.**

   The VPN Gateways form is displayed.
4. **Select the name of the VPN Gateway.**
5. **Under settings, select Authorization.**
6. **Select Application and click Add.**

   The Add Application Specific Entry form is displayed.
7. **In the Name field, enter a name for the entry and click Update.**
8. **In the System tree view, under Application, select Paths.**

The Application Specific Entry Paths form is displayed.



Application Specific Entries

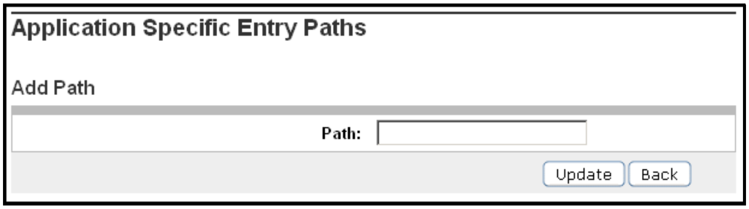
Used to specify a path to an intranet resource, e.g. to a specific folder on an FTP file server. The name of the application specific entry (as specified using the **Name** field) can later be referenced to make up one of the access rules for a specific user group..

ID	Name

No application specific entries configured.

9. **Click Add.**

   The Add Path form is displayed.



Application Specific Entry Paths

Add Path

Path:

10. **In the Path field, enter the desired path.**

    In this example the path to add is `/public`.

11. **Click Update.**

12. **Apply the changes.**

    This appspec definition in an access rule in the group configuration examples is referenced in the section “Group Configuration” on page 196.

Group Configuration

This section describes how to configure a group on the Avaya 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

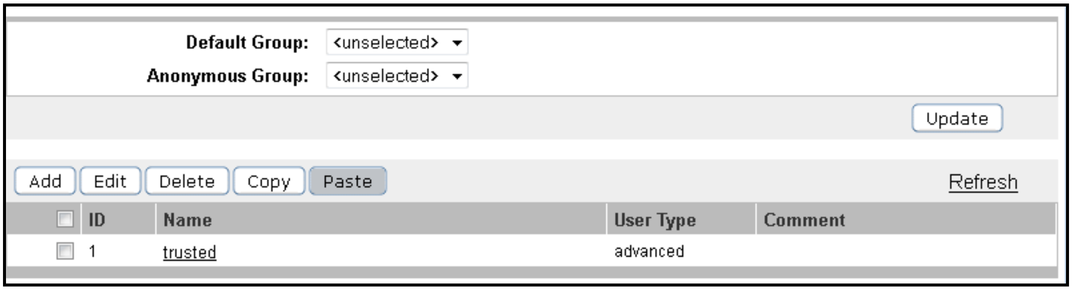
Configure Group 1

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on Groups settings.**

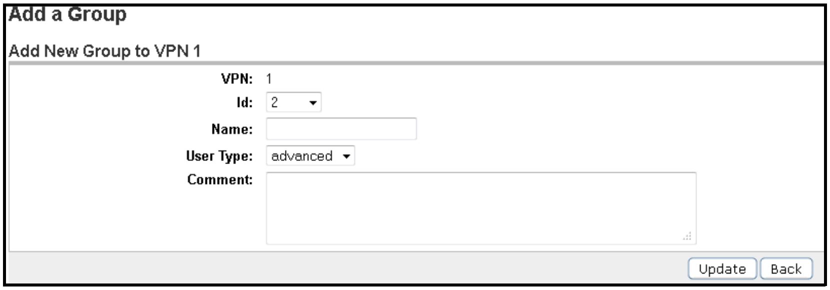


Default Group: <unselected>
Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

5. **Click Add.**

The Add a Group form is displayed.



Add a Group

Add New Group to VPN 1

VPN:	1
Id:	2
Name:	
User Type:	advanced
Comment:	

Some additional settings can be displayed in this form (Net Direct, Citrix Support and Wiper) if delegated from VPN level to group level. See the section “IE Cache Wiper” on page 181 and forward for more information.

6. **In the Name field, enter a name for the group.**

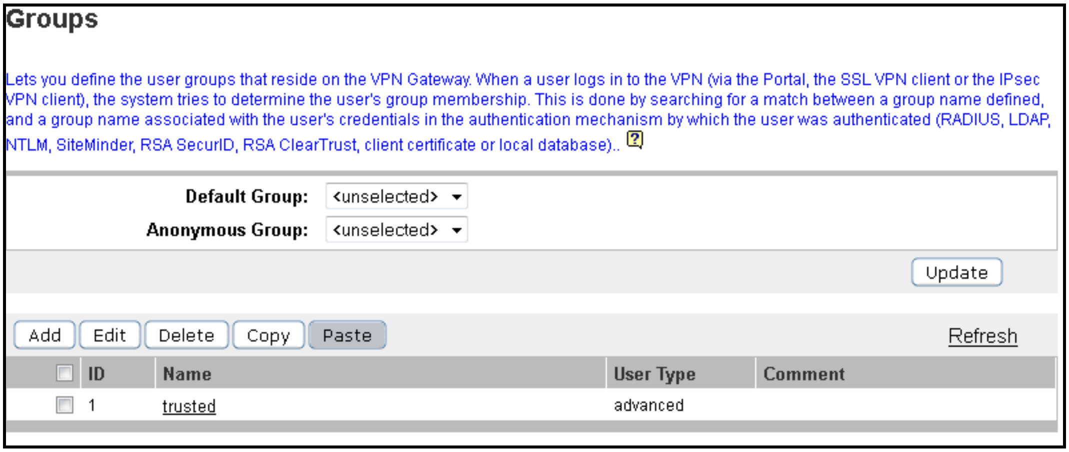
   When an external database is used for authentication (for example RADIUS), the group name assigned in the Avaya VPN Gateway configuration is matched against group names retrieved from the external authentication database.

7. **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.

8. **Click Update.**

   The Groups form is redisplayed with the new group added.



Groups

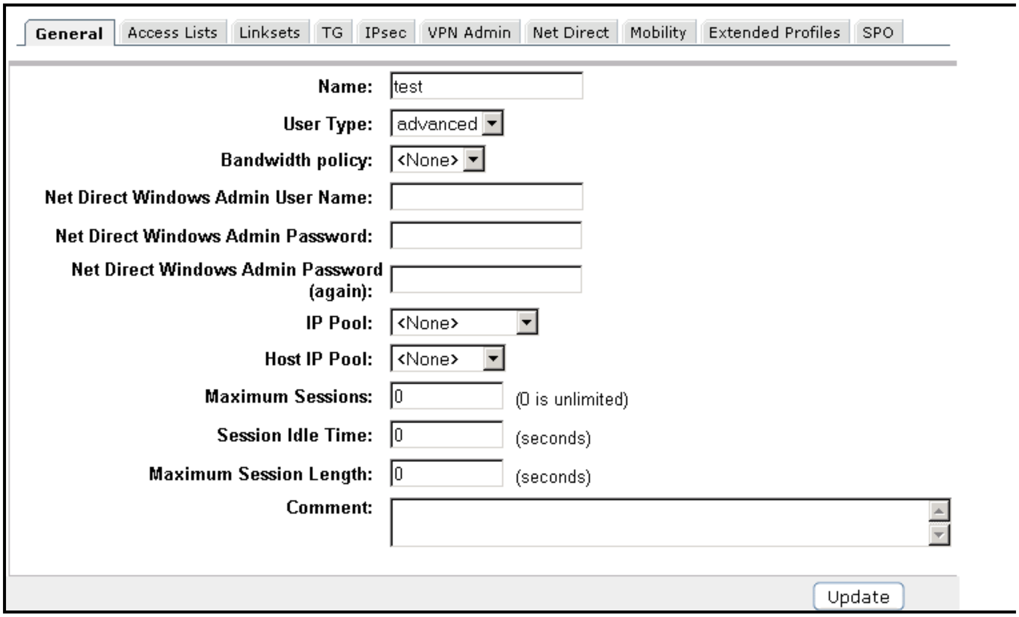
Lets you define the user groups that reside on the VPN Gateway. When a user logs in to the VPN (via the Portal, the SSL VPN client or the IPsec VPN client), the system tries to determine the user's group membership. This is done by searching for a match between a group name defined, and a group name associated with the user's credentials in the authentication mechanism by which the user was authenticated (RADIUS, LDAP, NTLM, SiteMinder, RSA SecurID, RSA ClearTrust, client certificate or local database)..

Default Group:	<unselected>
Anonymous Group:	<unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

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

   The Modify a Group form is displayed.



Name:	test
User Type:	advanced
Bandwidth policy:	<None>
Net Direct Windows Admin User Name:	
Net Direct Windows Admin Password:	
Net Direct Windows Admin Password (again):	
IP Pool:	<None>
Host IP Pool:	<None>
Maximum Sessions:	0 (0 is unlimited)
Session Idle Time:	0 (seconds)
Maximum Session Length:	0 (seconds)
Comment:	

   Now the form includes additional fields, e.g for mapping an IP Pool to the group and for configuring idle timeout and maximum session length. See the section "Number of Login Sessions" on page 180 and forward for explanations of available options.

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

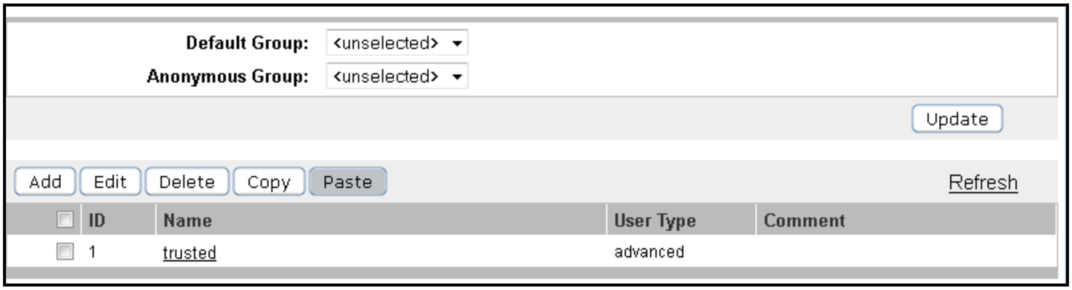
Configure Access Rule 1

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on Groups settings.**



Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

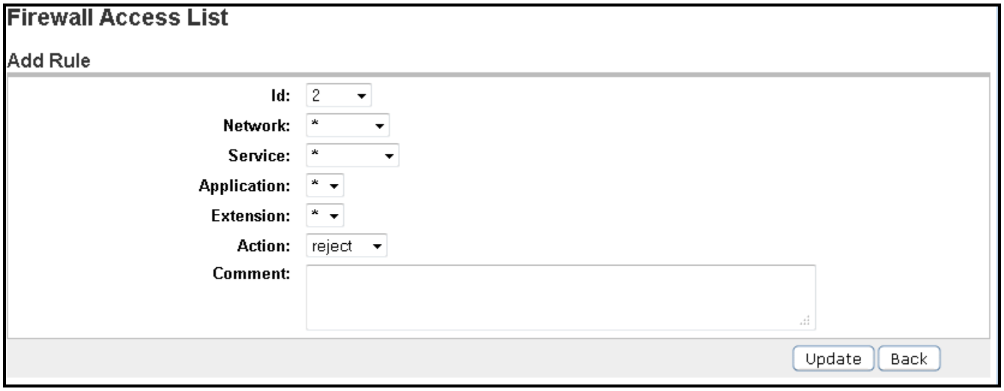
5. **Check the box against the Group name for which you want to view the firewall access list details and click Edit.**

6. **Click on Access List tab in Modify Group Name screen.**

7. **The Firewall Access List form is displayed.**

8. **Click Add to configure Access rule 1.**

   The Add Rule form is displayed.



Firewall Access List

Add Rule

Id: 2

Network: *

Service: *

Application: *

Extension: *

Action: reject

Comment:

9. **In the Network list box, select `owa`.**

   This step lets you reference the network definition created in the example in the section "Access to Outlook Web Access Server" on page 185, (i.e `owa`). It consists of a subnet definition identifying an Outlook Web Access server.

10. **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.

11. **Keep the asterisk (*) in the Application list box. This means that there are no restrictions to paths in the specified domain.**

12. **Finally, in the Action list box, select Accept.**

13. **Click Update.**

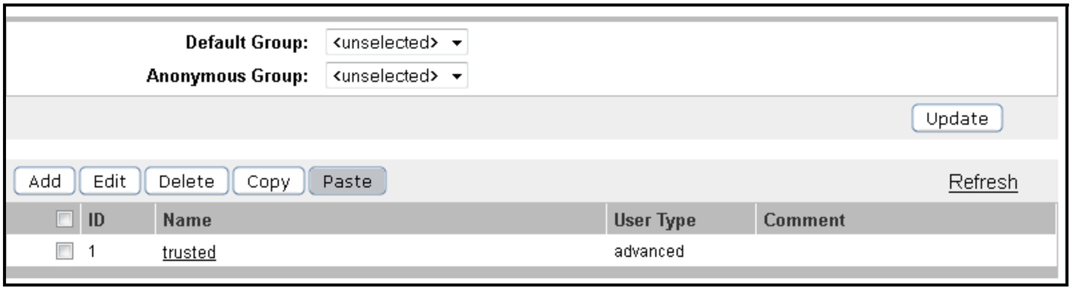
Configure Access Rule 2

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on Groups settings.**



Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

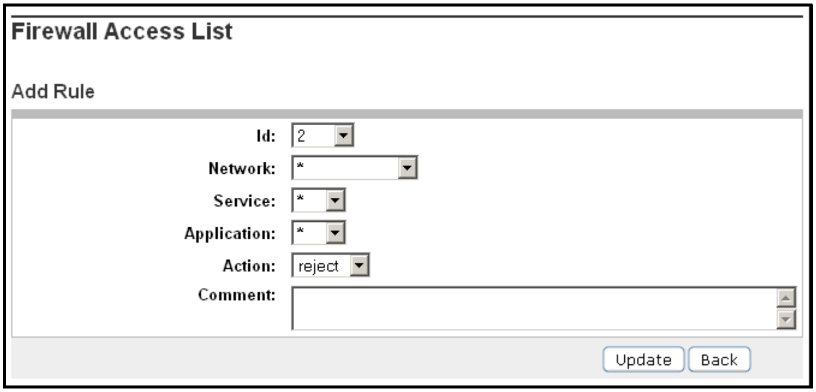
5. **Check the box against the Group name for which you want to view the firewall access list details and click Edit.**

6. **Click on Access List tab in Modify Group Name screen.**

7. **The Firewall Access List form is displayed.**

8. **Click Add to configure Access rule 2.**

The Add Rule form is displayed.



Firewall Access List

Add Rule

Id: 2
Network: *
Service: *
Application: *
Action: reject
Comment:

9. **In the Network list box, select `webserver`.**

   This step lets you reference the network definition created in the example in the section "Access to Outlook Web Access Server" on page 185, (i.e `owa`). It consists of a subnet definition identifying an Outlook Web Access server.

10. **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.

11. **In the Application list box, select `public`.**

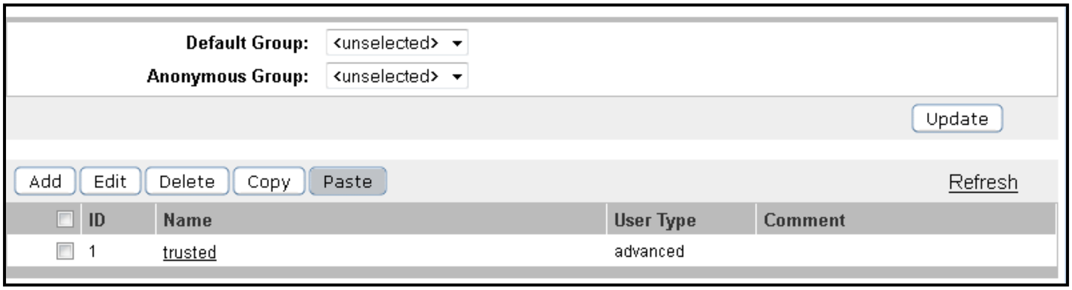
    This step lets you reference the application specific name we created in the example in the section "Access to Subfolder on Web Server" on page 193. This means that group members are only allowed access to the `/public` subfolder on the web server identified by the `webserver` network definition.

12. **Finally, in the Action list box, select Accept.**

13. **Click Update.**

Configure Access Rule 3.

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on Groups settings.**



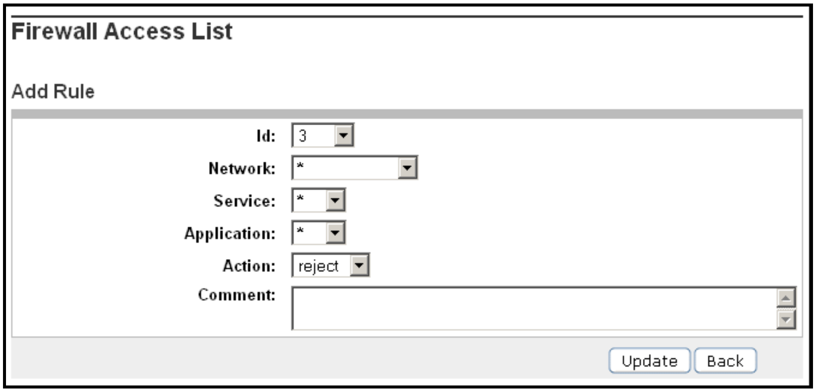
Default Group: <unselected>

Anonymous Group: <unselected>

☐	ID	Name	User Type	Comment
☐	1	trusted	advanced	

5. **Check the box against the Group name for which you want to view the firewall access list details and click Edit.**
6. **Click on Access List tab in Modify Group Name screen.**

   The Firewall Access List form is displayed.
7. **Click Add to configure Access rule 2.**



Firewall Access List

Add Rule

Id: 3

Network: *

Service: *

Application: *

Action: reject

Comment:

8. **In the Network list box, select `fileserver`.**

   This step lets you reference the network definition we created in the example in the section "Access to Intranet File Server" on page 188, i.e `fileserver`. It consists of a subnet definition identifying an FTP and SMB file server.

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

   This step lets you reference the `fileshare` service definition (created in the example in the section "Access to FTP and SMB Protocols" on page 192), corresponding to TCP port numbers 20, 21 and 139. It limits access to the FTP and SMB protocols.

10. **Keep the asterisk (*) in the Application list box. This means that there are no restrictions to paths in the specified domain.**

11. **Finally, in the Action list box, select Accept.**

12. **Click Update.**

13. **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.

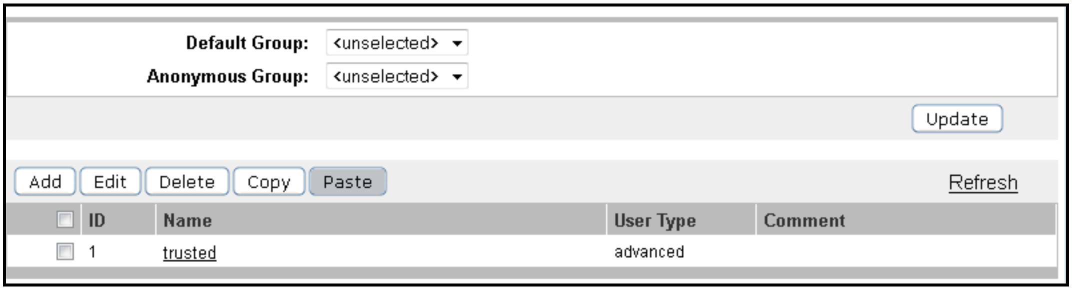
Access Allowed to Specific Subnet

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on Groups settings.**



Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

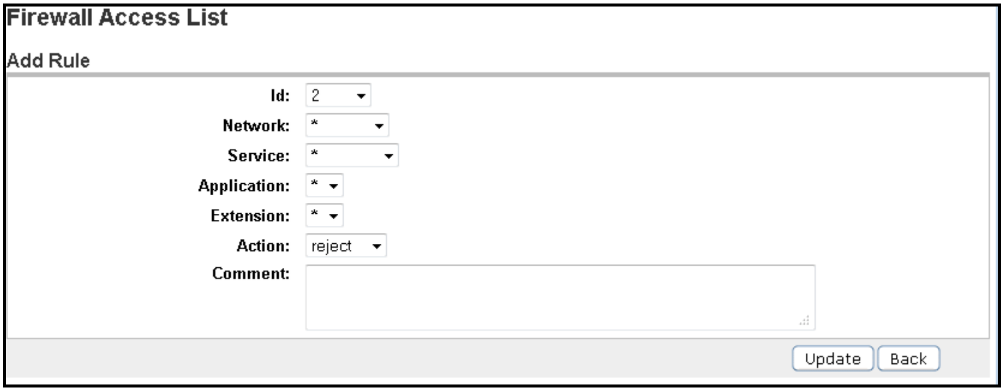
5. **Check the box against the Group name for which you want to view the firewall access list details and click Edit.**

6. **Click on Access List tab in Modify Group Name screen.**

   The Firewall Access List form is displayed.

7. **Click Add.**

   The Add Rule form is displayed.



Firewall Access List

Add Rule

Id: 2

Network: *

Service: *

Application: *

Extension: *

Action: reject

Comment:

8. **In the Network list box, select `sales`.**

   This step lets you reference the network definition we created in the example in the section "Access Allowed to Specific Subnet" on page 189, i.e `sales`.

9. **Keep the asterisks (*) in the Service and Application list boxes. This implies all port numbers, protocols and paths.**

10. **In the Action list box, select Accept.**

11. **Click Update.**

12. **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.

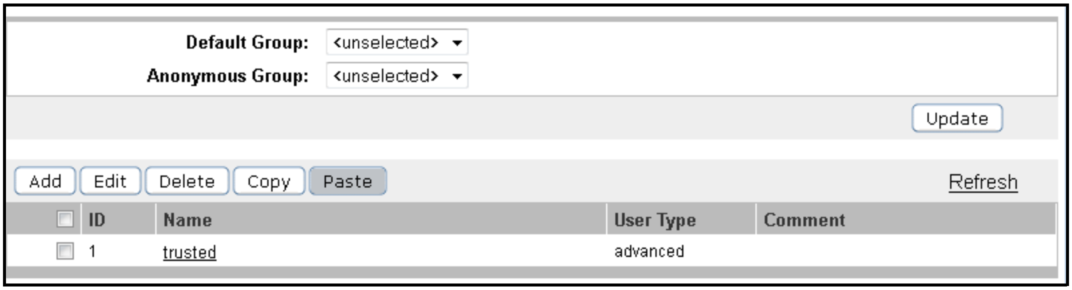
Access Rule 1: Access Denied to Specific Subdomain

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on Groups settings.**



Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

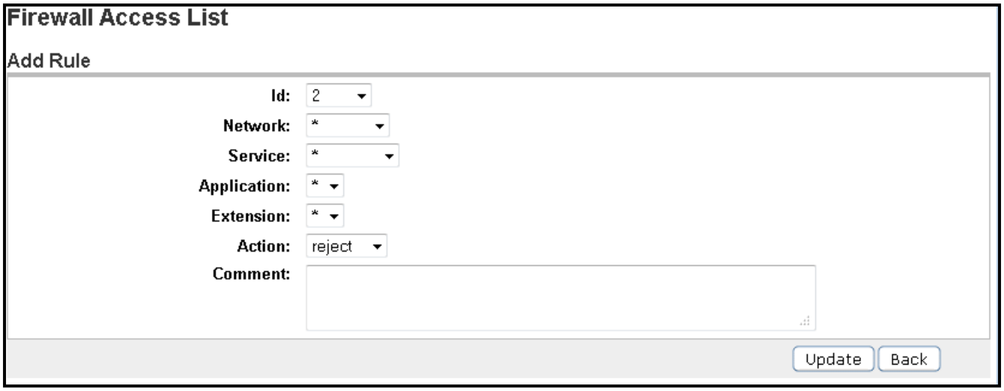
5. **Check the box against the Group name for which you want to view the firewall access list details and click Edit.**

6. **Click on Access List tab in Modify Group Name screen.**

   The Firewall Access List form is displayed.

7. **Click Add.**

   The Add Rule form is displayed.



Firewall Access List

Add Rule

Id: 2

Network: *

Service: *

Application: *

Extension: *

Action: reject

Comment:

8. **In the Network list box, select `secret`.**

   This step lets you reference the `secret` network definition (see the section "Access Denied to Specific Subnet" on page 190).

9. **Keep the asterisks (*) in the Service and Application list boxes. This implies all port numbers, protocols and paths.**

10. **In the Action list box, select `reject`.**

11. **Click Update.**

12. **Apply the changes.**

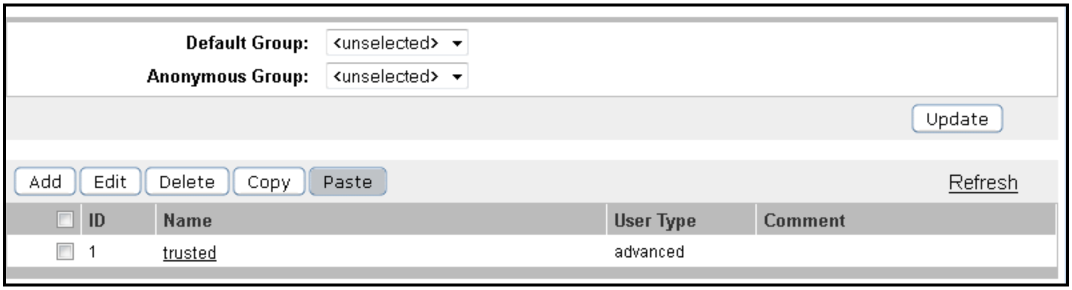
Access Rule 2: Access Allowed to All Hosts

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on Groups settings.**



Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

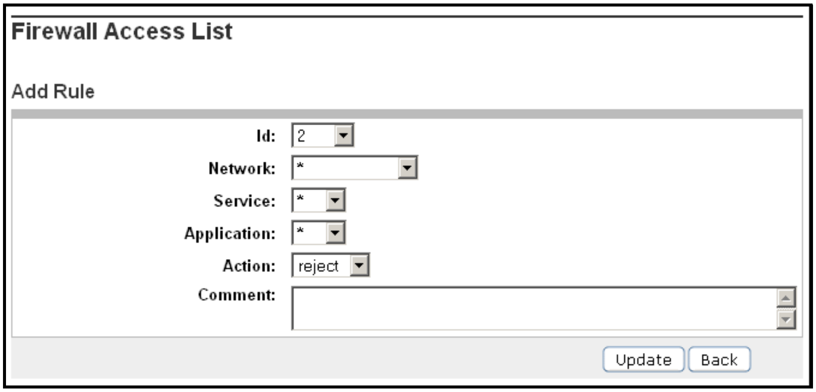
5. **Check the box against the Group name for which you want to view the firewall access list details and click Edit.**

6. **Click on Access List tab in Modify Group Name screen.**

   The Firewall Access List form is displayed.

7. **Click Add.**

   The Add Rule form is displayed.



Firewall Access List

Add Rule

Id:	2
Network:	*
Service:	*
Application:	*
Action:	reject
Comment:	

8. **Keep the asterisks (*) in the Network, Service and Application list boxes. This implies all networks, port numbers, protocols and paths.**

9. **In the Action list box, select Accept.**

10. **Click Update.**

11. **Apply the changes.**

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

All the data that can be defined 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, i.e. 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, Net Direct, or SPO)
- 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 (i.e. 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, i.e. 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 Avaya 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 8-1 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, i.e. 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 café 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, i.e. a branch office. When a group member connects to the VPN from the branch office network over the internet, that group member should have more generous access rights.

Define the Base Profile

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on Groups settings.**

   The Groups form is displayed.
5. **Click Add.**

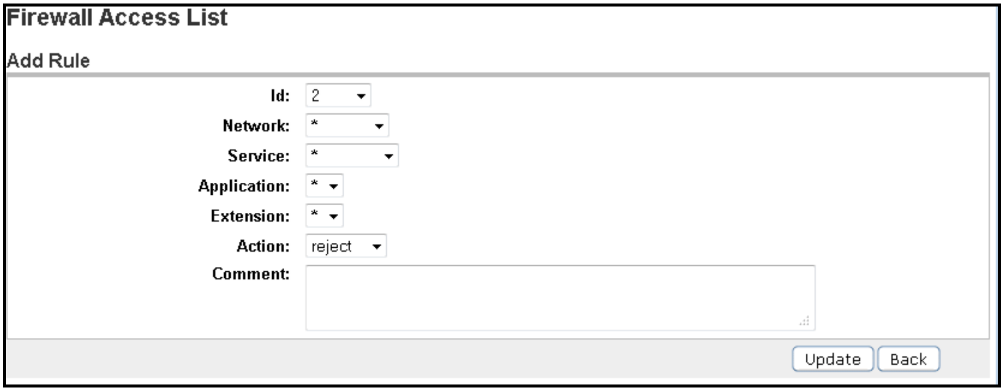
   The Add New Group form is displayed.
6. **In the Name field, enter the group name.**

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

   Select Advanced as user type.
8. **Click Update.**
9. **In the System tree view, expand Groups and select Access List.**

   The Firewall Access List form is displayed.
10. **In the VPN Number and Group list boxes, select the desired VPN and the user access group for which the access rule should be configured.**
11. **Click Refresh.**
12. **Click Add.**

The Add Rule form is displayed.



Firewall Access List

Add Rule

Id:	2
Network:	*
Service:	*
Application:	*
Extension:	*
Action:	reject
Comment:	

The next step is to specify the access rule pertaining to the base profile.

13. **In the Network list box, select `owa`.**

    This step lets you reference the network definition created in the example in the section "Access to Outlook Web Access Server" on page 185, (i.e `owa`). It consists of a subnet definition identifying an Outlook Web Access server.

14. **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.

15. **Keep the asterisk (*) in the Application list box. This implies all paths in the specified domain.**

16. **In the Action list box, select Accept.**

17. **Click Update.**

Define a Link for the Base Profile

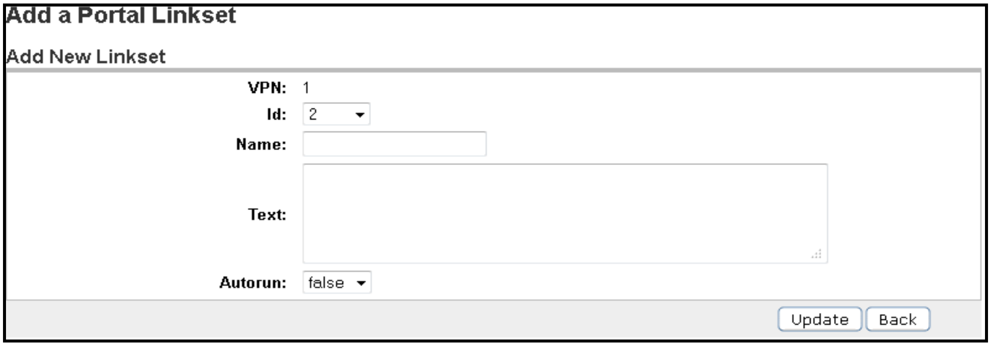
This example shows how to create a linkset with a link to the Outlook Web Access server. The link will be displayed on the Portal’s **Home** tab for the logged on group member.

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on Linksets settings.**

   The Portal Linksets form is displayed.

5. **Click Add.**

   The Add New Linkset form is displayed.



Add a Portal Linkset

Add New Linkset

VPN:	1
Id:	2
Name:	
Text:	
Autorun:	false

6. **In the Name field, enter the name `owa`.**

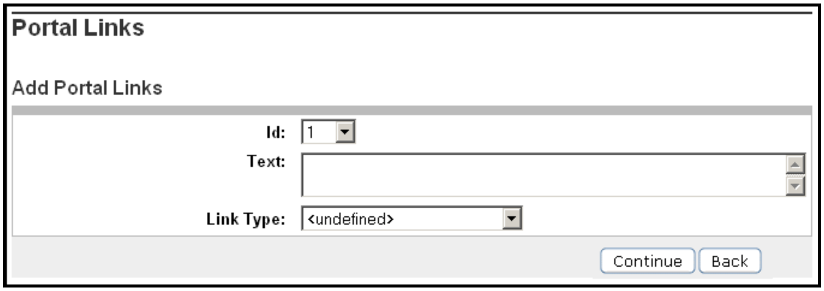
   We will later map this linkset name to the `staff` group.

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

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

8. **Click Update.**
9. **In the system tree view, select VPN Gateways.**
10. **Click on Linksets settings.**
11. **Check the box against the Linkset name for which you want to add a portal link and click Edit.**
12. **Click on the Portal Links tab and click Add.**

The Add Portal Links form is displayed.



Portal Links

Add Portal Links

Id: 1

Text:

Link Type: <undefined>

13. **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.

14. **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 Chapter 11, “Group Links”.

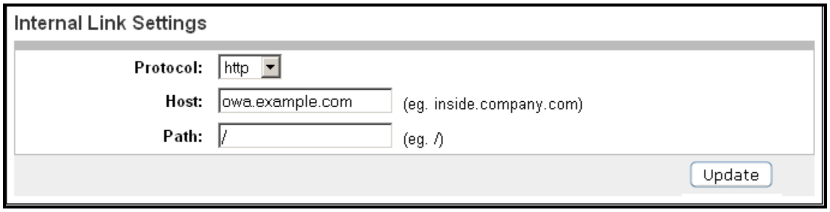
15. **Click Continue.**

    The Internal Website Links form is displayed.

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

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

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



Internal Link Settings

Protocol: http

Host: owa.example.com (eg. inside.company.com)

Path: / (eg. /)

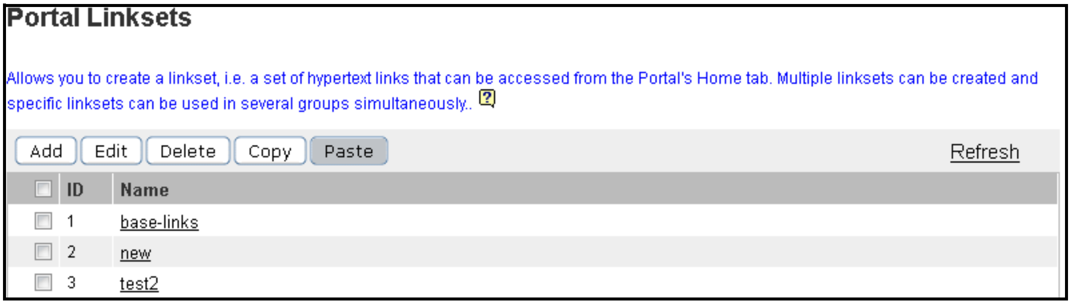
19. **Click Update.**

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 in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on Linksets settings.**

   The Portal Linksets form is displayed.



Portal Linksets

Allows you to create a linkset, i.e. a set of hypertext links that can be accessed from the Portal's Home tab. Multiple linksets can be created and specific linksets can be used in several groups simultaneously..

□	ID	Name
□	1	base-links
□	2	new
□	3	test2

5. **In the Portal Linksets list box, select the linkset that should be mapped to the current group, i.e. `owa`.**
6. **Click Add.**
7. **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.

The Add Network form is displayed.

1. **Log on to the BBI as system administrator.**
2. **Click on Config Tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Under Settings, select Authorization.**
5. **Click Add.**

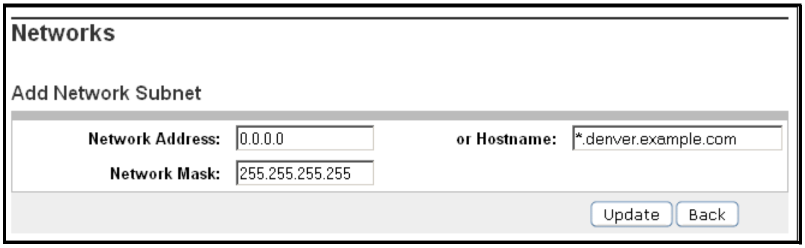
   The Add Network form is displayed.
6. **In the Name field, enter the network name.**

   In this example the network is called `branchoffice`.
7. **Click Continue.**

   The form is expanded.
8. **Under Network Subnets, click Add.**

   The Add Network Subnet form is displayed.
9. **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.



Networks

Add Network Subnet

Network Address: 0.0.0.0

Network Mask: 255.255.255.255

or Hostname: *.denver.example.com

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

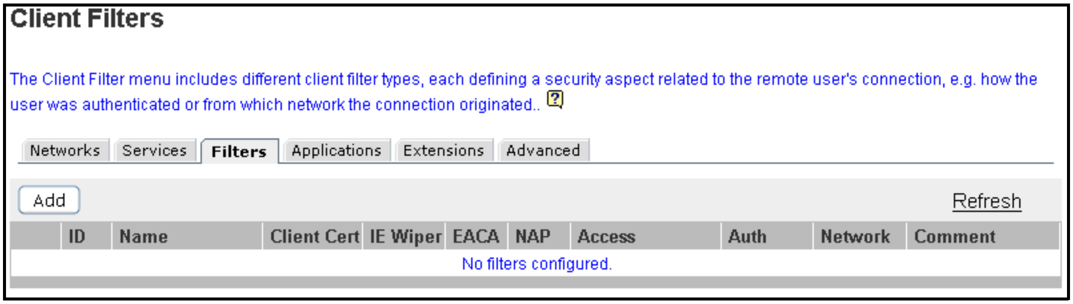
Define a Client Filter Referencing the Client Network

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. **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.



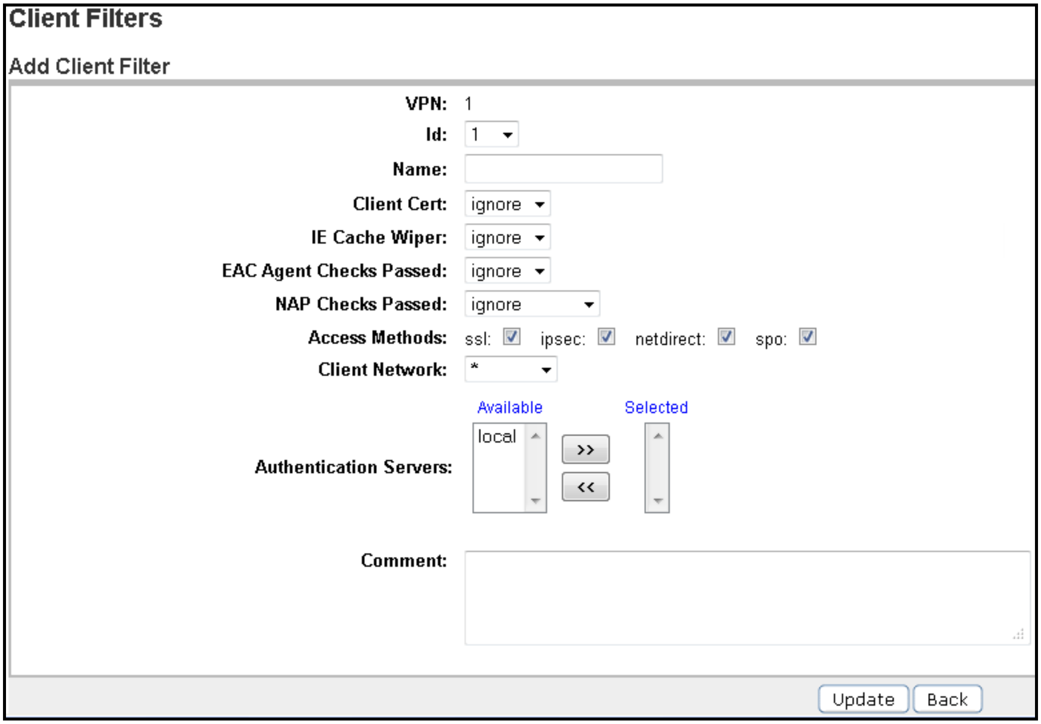
Client Filters

The Client Filter menu includes different client filter types, each defining a security aspect related to the remote user's connection, e.g. how the user was authenticated or from which network the connection originated.. ?

	ID	Name	Client Cert	IE Wiper	EACA	NAP	Access	Auth	Network	Comment
No filters configured.										

5. **Click Add.**

The Add Client Filter form appears.



Client Filters

Add Client Filter

VPN: 1

Id: 1

Name:

Client Cert: ignore

IE Cache Wiper: ignore

EAC Agent Checks Passed: ignore

NAP Checks Passed: ignore

Access Methods: ssl: ☑ ipsec: ☑ netdirect: ☑ spo: ☑

Client Network: *

Authentication Servers: Available: local Selected:

Comment:

6. **In the Name field, enter the client filter’s name.**

   In this example we will call the filter branchoffice.

7. **In the Client Network list box, select the network created in the section “Create a Network Identifying the Branch Office Network” on page 216, i.e. branchoffice.**

8. **Click Update.**

9. **Apply the changes.**

Define the Extended Profile

Now it is time to define the extended profile. The extended profile is triggered when the group member accesses the Portal from the network referenced in the extended profile’s client filter.

Because the user is connecting from a secure network, more generous access rules can be presented to the user.

1. **Log on to the BBI as system administrator.**

2. **Click on Config Tab.**

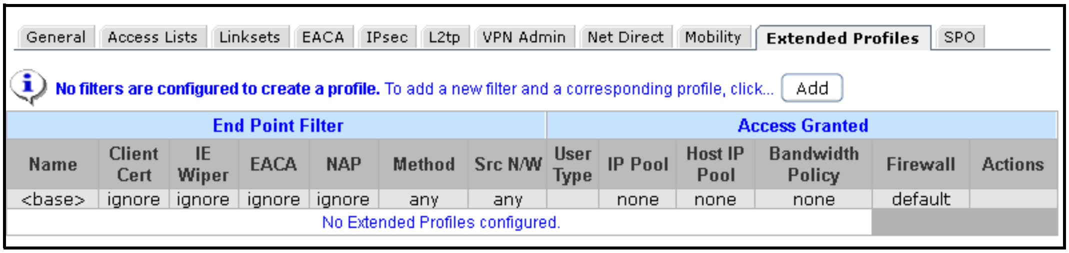
3. **In the system tree view, select VPN Gateways.**

4. **Under Settings, select Groups.**

5. **Click a group name.**

6. **Click on Extended Profile.**

   The Extended Profiles form is displayed.



General | Access Lists | Linksets | EACA | IPsec | L2tp | VPN Admin | Net Direct | Mobility | **Extended Profiles** | SPO

No filters are configured to create a profile. To add a new filter and a corresponding profile, click... Add

End Point Filter							Access Granted					
Name	Client Cert	IE Wiper	EACA	NAP	Method	Src N/W	User Type	IP Pool	Host IP Pool	Bandwidth Policy	Firewall	Actions
<base>	ignore	ignore	ignore	ignore	any	any		none	none	none	default	
No Extended Profiles configured.												

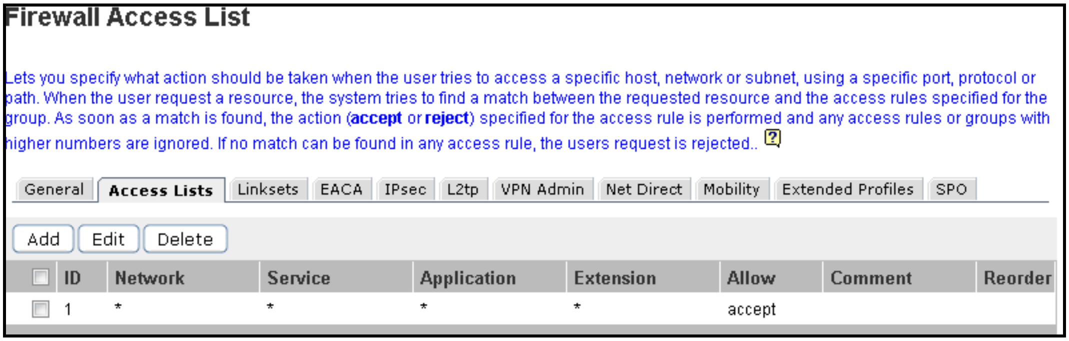
7. **Click Add.**

   The client filters are added to the in the table.

8. **Click on the Modify button** ✎ **in the table.**

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

   Extended Access List form is displayed.



Firewall Access List

Lets you specify what action should be taken when the user tries to access a specific host, network or subnet, using a specific port, protocol or path. When the user request a resource, the system tries to find a match between the requested resource and the access rules specified for the group. As soon as a match is found, the action (**accept** or **reject**) specified for the access rule is performed and any access rules or groups with higher numbers are ignored. If no match can be found in any access rule, the users request is rejected.. ?

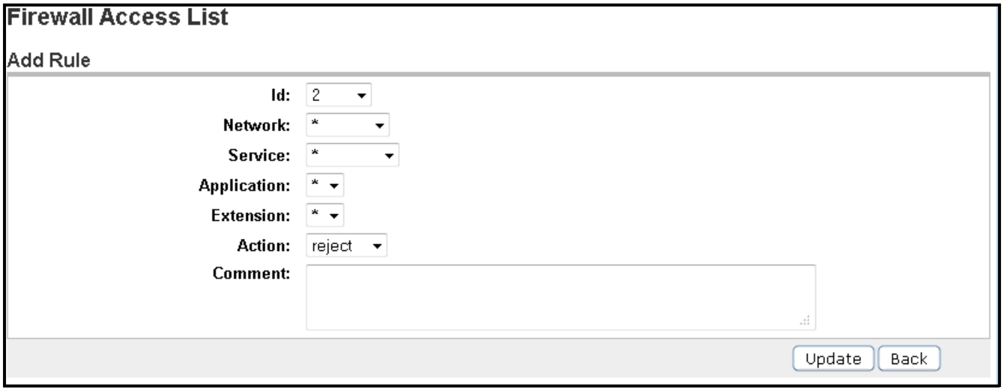
General | **Access Lists** | Linksets | EACA | IPsec | L2tp | VPN Admin | Net Direct | Mobility | Extended Profiles | SPO

Add | Edit | Delete

□	ID	Network	Service	Application	Extension	Allow	Comment	Reorder
□	1	*	*	*	*	accept		

10. **Click Add.**

The Add Rule form is displayed for you to specify Access rule 1, allowing access to all networks and protocols.



Firewall Access List

Add Rule

Id:	2
Network:	*
Service:	*
Application:	*
Extension:	*
Action:	reject
Comment:	

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.**

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, i.e. 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 Chapter 11, "Group Links".

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

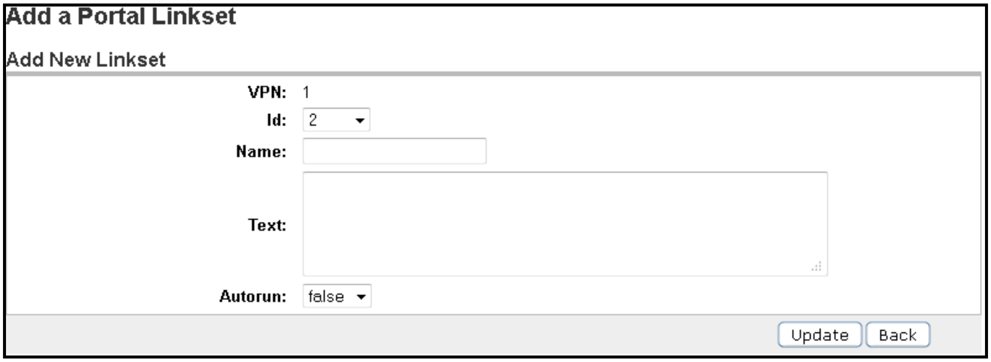
3. **Click on the VPN gateway name.**

4. **Click on Linksets settings.**

   The Portal Linksets form is displayed.

5. **Click Add.**

The Add New Linkset form is displayed.



Add a Portal Linkset

Add New Linkset

VPN: 1

Id: 2

Name:

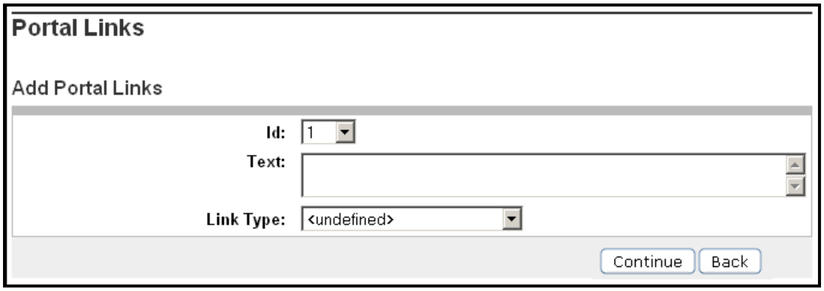
Text:

Autorun: false

6. **In the Name field, enter the name `ftp`.**
7. **In the Text field, enter a heading for the linkset (optional).**

   The linkset heading is displayed above the links contained in the linkset.
8. **Click Update.**
9. **In the system tree view, select VPN Gateways.**
10. **Click on Linksets settings.**
11. **Check the box against the Linkset name for which you want to add a portal link and click Edit.**
12. **Click on the Portal Links tab and click Add.**

    The Add Portal Links form is displayed.



Portal Links

Add Portal Links

Id: 1

Text:

Link Type: <undefined>

13. **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.

14. **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 Chapter 11, “Group Links”.

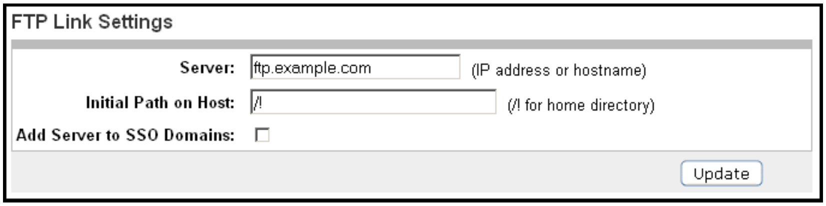
15. **Click Continue.**

    The Portal Links form is expanded.

16. **Under FTP Link Settings, in the Server field, enter the IP address or hostname of the FTP server.**

    In this example we will enter the host name `ftp.example.com`.

17. **In the Initial Path on Host field, enter /! to specify the home directory.**



FTP Link Settings

Server: ftp.example.com (IP address or hostname)

Initial Path on Host: /! (/! for home directory)

Add Server to SSO Domains: □

18. **Click Update.**

Map the Linkset to the Extended Profile

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

1. **Log on to the BBI as administrator user.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN name from the Name list.**

   The VPN Summary screen is displayed.

5. **Select the Groups from the settings.**

   The Groups screen is displayed.

6. **Select the name from the list.**

   Modify a Group form is displayed.

7. **Select the Extended Profiles.**

The Extended Profiles screen is displayed.

8. **Click Add Profile.**

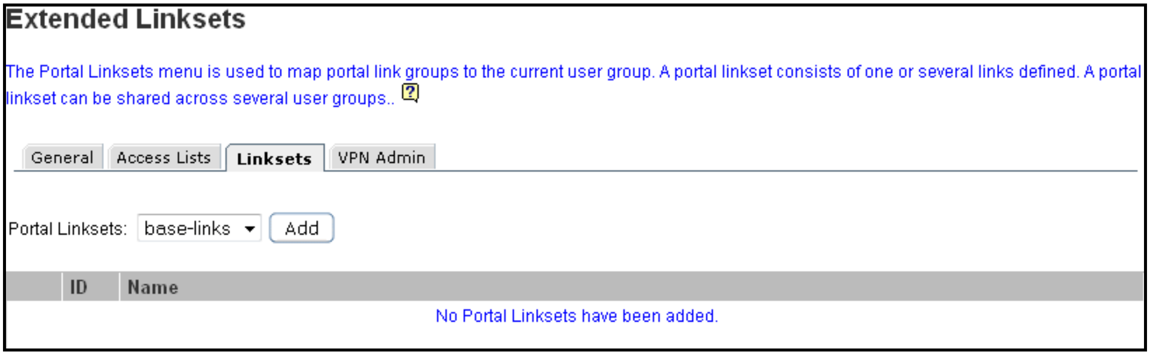
   The Extended Profiles screen is displayed with modify button enabled in Actions.

9. **Click Modify button in the table.**

   The General settings of the Current Extended Profiles screen is displayed.

10. **Select the Linksets.**

    The Extended Linksets form is displayed.



Extended Linksets

The Portal Linksets menu is used to map portal link groups to the current user group. A portal linkset consists of one or several links defined. A portal linkset can be shared across several user groups..

Portal Linksets: base-links

ID	Name
No Portal Linksets have been added.	

11. **In the Portal Linksets list box, select the portal linkset that you wish to map to the current extended profile.**

    In this example, we will select the base-links.

12. **Click Add and 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 café:** 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 café's network. Only the linkset mapped to the base profile (i.e. 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 Avaya VPN Gateway's 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 Group Settings.**

   The Groups form is displayed.
3. **Click Add.**

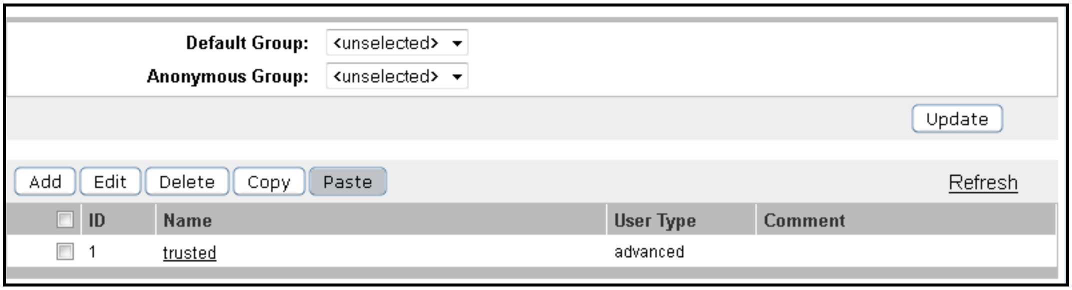
   The Add New Group form is displayed.
4. **In the Name field, enter a name for the group.**

   In this example, name the group `engineer`.
5. **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.
6. **Click Update.**

Configure the Base Profile’s Access Rules

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on Groups settings.**



Default Group: <unselected>

Anonymous Group: <unselected>

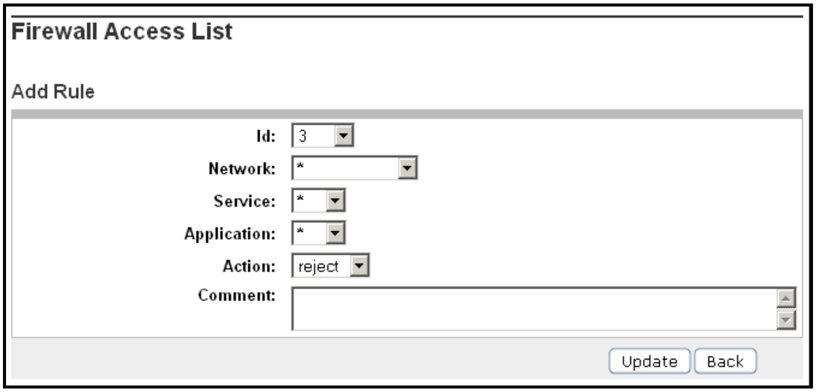
□	ID	Name	User Type	Comment
□	1	trusted	advanced	

5. **Check the box against the Group name for which you want to view the firewall access list details and click Edit.**

6. **Click on Access List tab in Modify Group Name screen.**

   The Firewall Access List form is displayed.

7. **Click Add to configure Access rule.**



Firewall Access List

Add Rule

Id: 3

Network: *

Service: *

Application: *

Action: reject

Comment:

8. **In the Network list box, select the `sales` network definition.**

   In this example we will make use of the network definition we created in the example in section "Access Allowed to Specific Subnet" on page 189, i.e. `sales`.

9. **Keep the asterisk (*) in the Service and Application list boxes. This implies all services and paths.**

10. **In the Action list box, select Accept.**

11. **Click Update.**

Create a Linkset with a Link to the Intranet Web Server

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

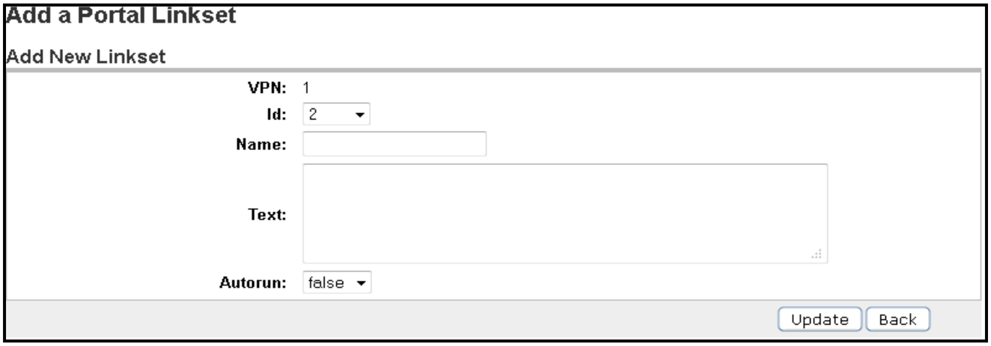
3. **Click on the VPN gateway name.**

4. **Click on Linksets settings.**

   The Portal Linksets form is displayed.

5. **Click Add.**

   The Add New Linkset form is displayed.



Add a Portal Linkset

Add New Linkset

VPN:	1
Id:	2
Name:	
Text:	
Autorun:	false

6. **In the Name field, enter the name `intranet`.**

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

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

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

8. **Click Update.**

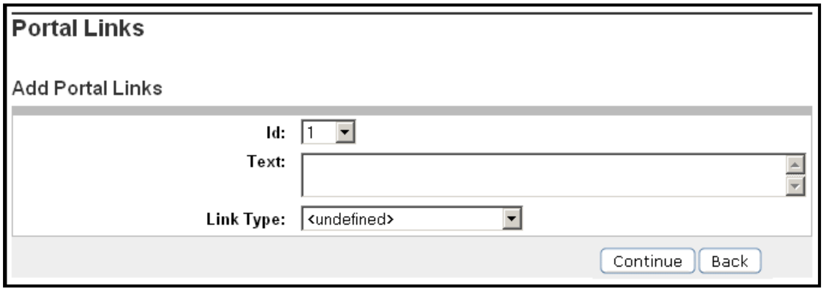
9. **In the system tree view, select VPN Gateways.**

10. **Click on Linksets settings.**

11. **Check the box against the Linkset name for which you want to add a portal link and click Edit.**

12. **Click on the Portal Links tab and click Add.**

    The Add Portal Links form is displayed.



Portal Links

Add Portal Links

Id: 1

Text:

Link Type: <undefined>

13. **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.

14. **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 Chapter 11, "Group Links".

15. **Click Continue.**

    The Portal Links form is expanded.

16. **Under Internal Link Settings, in the Protocol list box, select the desired protocol, in this example `http`.**

17. **In the Host field, enter `inside.example.com` as the web server's address.**

18. **In the Path field, enter forward slash (/) to imply the web server's root.**

19. **Click Update.**

Map the Linkset to the Base Profile

1. **In the System tree view, select VPN Gateways.**

2. **Click on the VPN gateway name.**

3. **Select Linksets.**

   The Portal Linksets form is displayed.

4. **In the VPN Number and Group list boxes, select the desired VPN and user access group. Click Refresh following each selection.**

5. **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.

6. **Click Add.**

7. **Apply the changes.**

Configure RADIUS Authentication

For instructions on how to configure RADIUS authentication on the Avaya VPN Gateway, see the section "RADIUS Authentication" on page 242 in Chapter 9, "Authentication Methods".

Define the Client Filter

Before you create the extended profile you should define the client filter. The client filter should later be referenced in the extended profile. The extended profile in its turn should be triggered when a group member authenticates via the RADIUS server.

1. **In the System tree view, select VPN gateways.**

2. **Select the name of the VPN gateway.**

3. **Under settings, select Authorization.**

4. **Click Filters tab.**

5. **Click Add.**

   The Add Client Filter form is displayed.

6. **In the Name field, enter radius as the client filter name.**

7. **In the Authentication Servers box, under Available, select radius.**

   In this example we assume that radius is the name given to this authentication mechanism when it was configured.

8. **Move the selected authentication server name to the right box (under Selected) by clicking the >> button.**

9. **Click Update.**

10. **Apply the changes.**

Configure the Extended Profile

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. **Click on the VPN name.**

3. **Select Group Settings and select Extended Profiles.**

   The Extended Profile Extensions form is displayed.

4. **In the VPN Number and Group list boxes, select the desired VPN and the user access group for which you wish to create an extended profile. Click Refresh.**

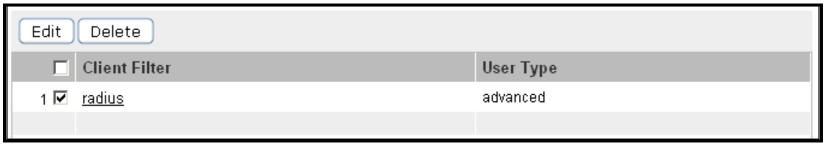
5. **In the Client Filter list box, select `radius`.**

   This is the client filter we created in the previous section.

6. **Click Add.**

   The client filter is mapped to the current extended profile.

7. **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.**



	☐	Client Filter	User Type
1	☑	radius	advanced

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

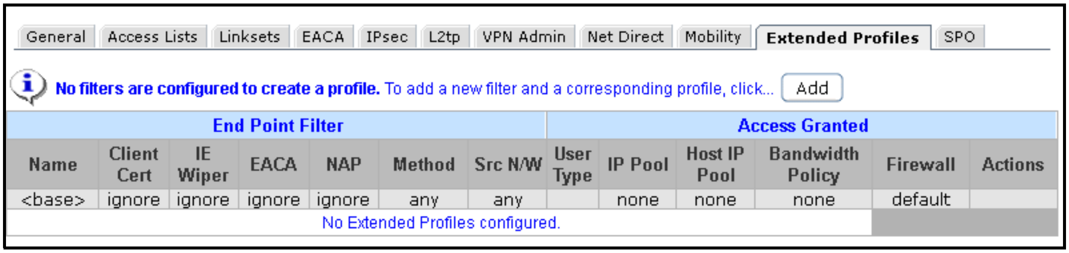
8. **Click Update.**

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. **Log on to the BBI as system administrator.**
2. **Click on Config Tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Under Settings, select Groups.**
5. **Click on Extended Profile.**

   The Extended Profiles form is displayed.



General | Access Lists | Linksets | EACA | IPsec | L2tp | VPN Admin | Net Direct | Mobility | **Extended Profiles** | SPO

No filters are configured to create a profile. To add a new filter and a corresponding profile, click... Add

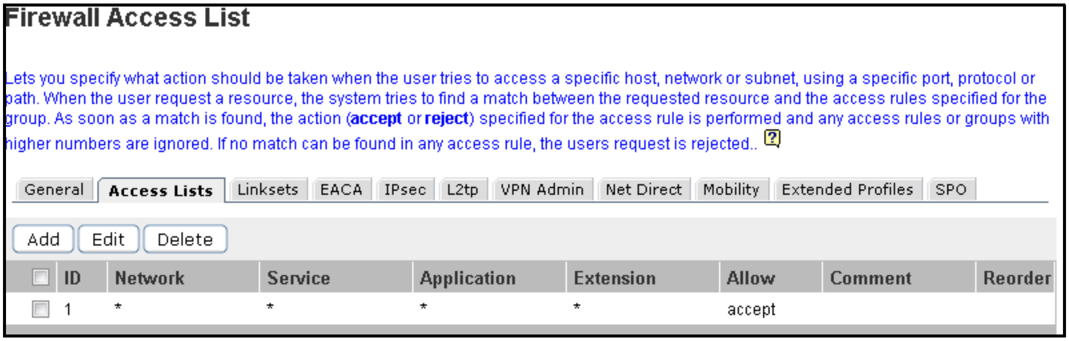
End Point Filter							Access Granted					
Name	Client Cert	IE Wiper	EACA	NAP	Method	Src N/W	User Type	IP Pool	Host IP Pool	Bandwidth Policy	Firewall	Actions
<base>	ignore	ignore	ignore	ignore	any	any		none	none	none	default	
No Extended Profiles configured.												

6. **Click Add Profile.**

   The extended profile will be added to the in the table.

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

Extended Access List form is displayed.



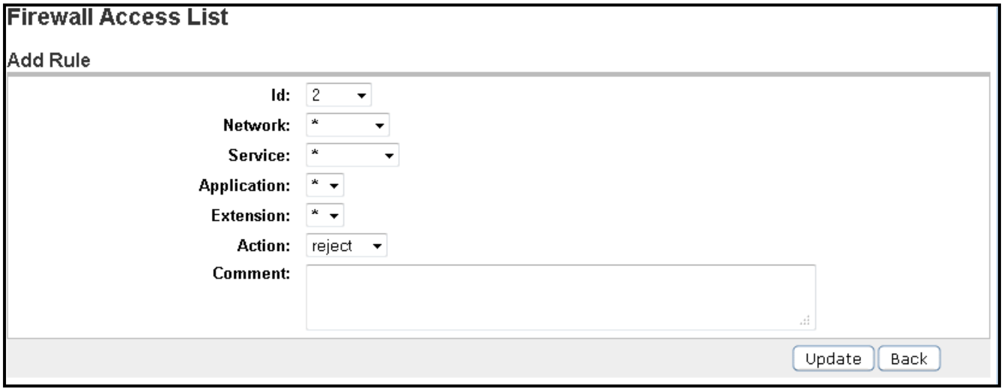
Firewall Access List

Lets you specify what action should be taken when the user tries to access a specific host, network or subnet, using a specific port, protocol or path. When the user request a resource, the system tries to find a match between the requested resource and the access rules specified for the group. As soon as a match is found, the action (**accept** or **reject**) specified for the access rule is performed and any access rules or groups with higher numbers are ignored. If no match can be found in any access rule, the users request is rejected..

□	ID	Network	Service	Application	Extension	Allow	Comment	Reorder
□	1	*	*	*	*	accept		

9. **Click Add.**

   The Add Rule form is displayed for you to specify Access rule 1, allowing access to all networks and protocols.



Firewall Access List

Add Rule

Id:	2
Network:	*
Service:	*
Application:	*
Extension:	*
Action:	reject
Comment:	

10. **Click Add.**

    The Add Rule form is displayed.

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 Chapter 11, “Group Links”.

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 Profiles for Users with Client Certificate and IE Cache Wiper

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.

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 logs in to the Portal from a computer for the first time, he is asked whether or not to install the cache wiper. The IE Cache Wiper clears HTML pages cached during a Portal session. In addition, the Portal address is removed from the 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 remote users *without* a client certificate 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 VPN Gateway name.**
3. **Under Settings, select Groups.**
4. **Select the Group name from the list.**
5. **Click on Extended Profiles tab.**

   Extended Profiles screen is displayed.
6. **To add a profile, click Add Profile.**
7. **Enter the base name.**
8. **In the Client Cert list box, select Yes.**
9. **In the IE Wiper list box, select Yes.**

10. **Click Update.**

11. **In the system tree view, select VPN Gateways.**

12. **Select the VPN Gateway name.**

13. **Under Settings, select Authorization.**

14. **Click on Filters tab.**

    The End point filters that you specified in the table under Extended Profiles form is displayed here.

Extended Profile for Users with Specific Access Method

A client filter can also identify the remote user's access method, i.e. 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 and the *installable* Avaya VPN Client (not the Net Direct client).
- IPsec refers to access through the Avaya VPN Client.
- Net Direct refers to access through the Net Direct client.
- SPO client refers to access through the SPO client.

For more information about the Avaya VPN Client see Chapter 21, "Transparent Mode". For more information about the Net Direct client, see Chapter 7, "Net Direct".

Extended Profile for Users Subject to a 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 Chapter 15, "Configure Avaya Endpoint Access Control Agent".

Avaya Endpoint Access Control Agent

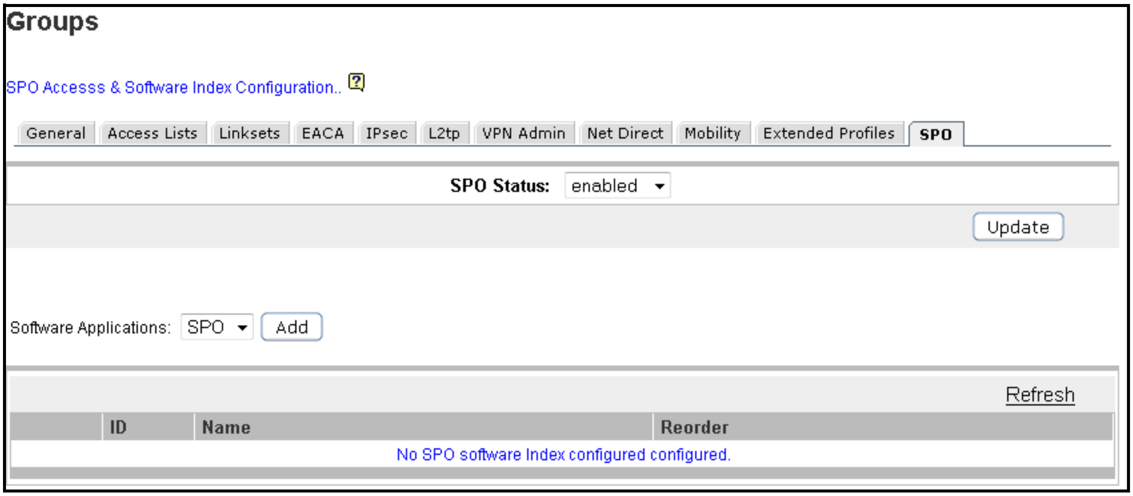
Adding a Secure Portable Office software index

This section describes how to configure the Secure Portable Office (SPO) client and to add software indexes to the Client. When the SPO is enabled under groups, the software is available for download on the portal. For more information on SPO client see, Chapter 13, “Secure Portable Office Client”.

1. **Login as system administrator.**
2. **Select Config tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Select the VPN Gateway name.**

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

   By default, General tab is selected.
6. **Select SPO tab.**



Groups

SPO Accesss & Software Index Configuration..

SPO Status: enabled

Software Applications: SPO

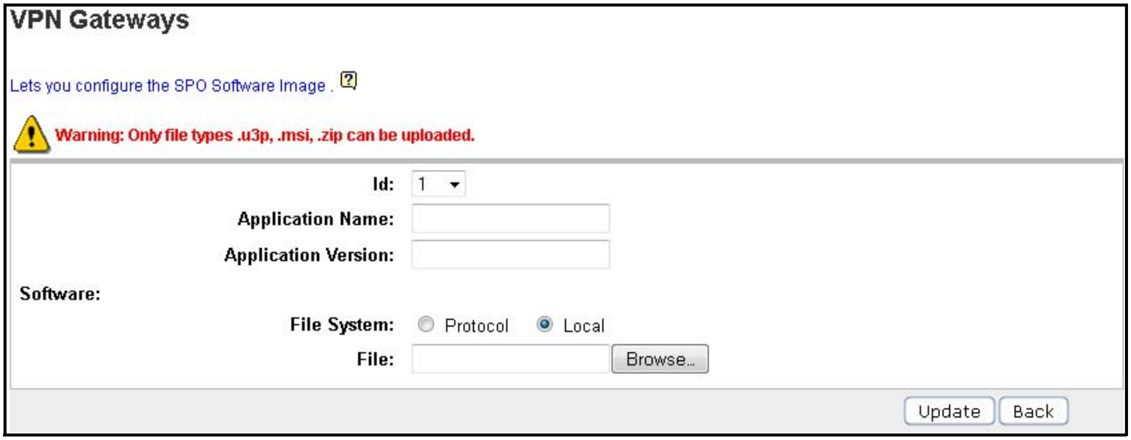
ID	Name	Reorder
No SPO software Index configured configured.		

7. **Select the SPO status as enabled.**

   To access the software, ensure the SPO Status is enabled.

8. **Click Update.**

9. **Click Add to add an SPO software index.**



VPN Gateways

Lets you configure the SPO Software Image .

Warning: Only file types .u3p, .msi, .zip can be uploaded.

Id: 1

Application Name:

Application Version:

Software:

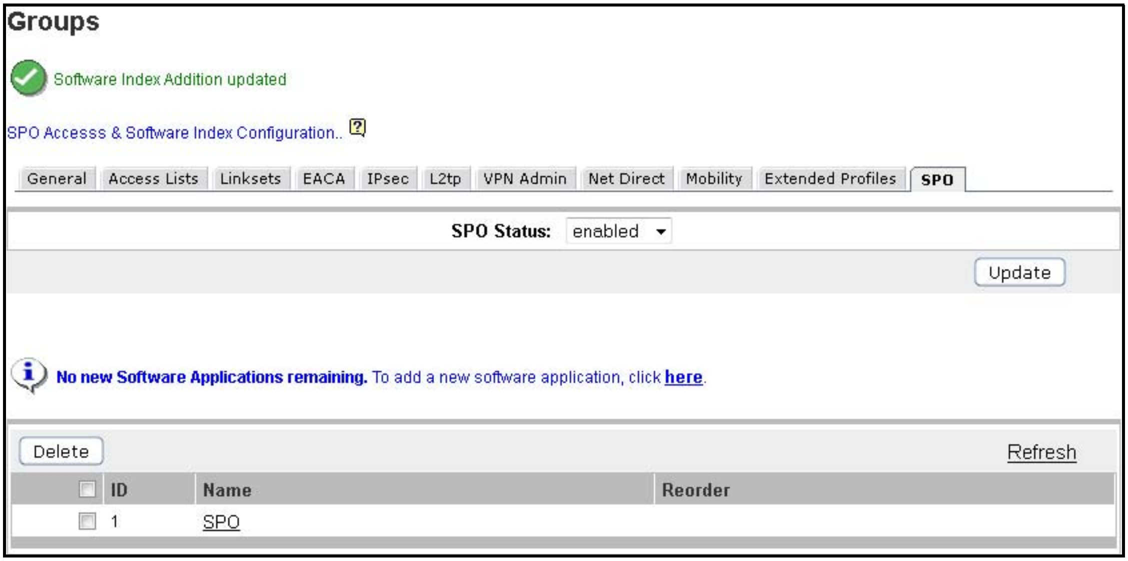
File System: ○ Protocol ● Local

File:

NOTE – A warning message “`A Software Application is required for this page. Click here to configure a Software Application.`” is displayed during SPO software index configuration.

10. **Click Update.**

The newly created SPO software index is added to the list.



Groups

Software Index Addition updated

SPO Accesss & Software Index Configuration..

SPO Status: enabled

No new Software Applications remaining. To add a new software application, click here.

	ID	Name	Reorder
□	1	SPO	

11. **To move a link up or down in the list, click the arrows in the Reorder column.**

12. **Click Update and click Apply to apply the changes.**

CHAPTER 9
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
- HTTP

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 SecurID or RSA ClearTrust server. This makes it possible to use already existing authentication databases within the intranet. The Avaya 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.

The authentication subsystem caches responses given to queries sent to the external databases. The TTL for the cache is the same as the idle timeout. The cache significantly relieves the burden put on the external databases.

Local Database Authentication

The Avaya VPN Gateway 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 Avaya 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 in section "Local Database Authentication" on page 321.

Client Certificate Authentication

With client certificate authentication enabled on the Avaya VPN Gateway, no Portal login is required for remote SSL users with a valid client certificate installed on their computers. Once the Avaya 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, users with the Avaya VPN Client can authenticate to the VPN through client certificate authentication once the client certificate has been selected in the Avaya VPN Client.

Client certificate authentication is described in section "Client Certificate Authentication" on page 335.

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 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.

NOTE – The RSA SecurID New Pin mode is not supported when using Secondary Authentication service.

To view a **Secondary Authentication Server** selection example, see “Configure Advanced settings” on page 348 .

Avaya VPN Client authentication types

The following table describes supported Avaya VPN Client authentication methods when using client authentication types:

Table 9-1 Avaya VPN Client authentication types

Authentication type	Supported method
Username and password	Enter a username and password only for Local Database authentication. A username and password does not work with RADIUS, LDAP and other authentication methods.
Certificate	Use the certificate type for certificate authentication and, beginning with Release 9.0, Two Factor Authentication (certificate plus username and password).
Group security	
Group password	Use a Group password when configuring Group security for a Local Database, RADIUS, LDAP and other authentication methods except certificate or RSA SecurID. For this type of configuration to work, enter additional credentials for Group ID and Group password as well as the username and password. The Group ID is the same as the Group name configured on the AVG. Configure the Group password, which is the Shared Secret, at Group level on the AVG in the same menu as the user tunnel profile.
Challenge Response Token	Use the Token for hardware or software Token authentication, for example, RSA SecurID. Token options also require a Group ID and Group password.
Response only Hardware Token	
Response only Software Token	

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 system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

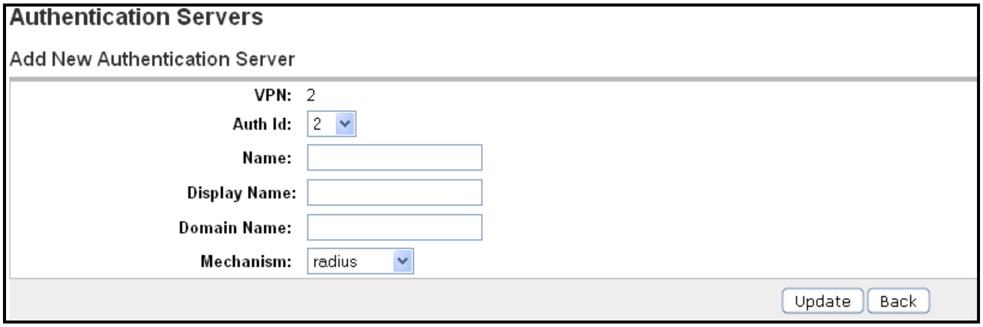
4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

   Authentication Server screen is displayed.

6. **Click Add.**

   Add New Authentication server is displayed.



Authentication Servers

Add New Authentication Server

VPN: 2

Auth Id: 2

Name:

Display Name:

Domain Name:

Mechanism: radius

7. **Select the Auth ID.**

8. **In the Name field, enter the Authentication server name.**

   A name is mandatory with not more than 30 alphanumeric characters. If the current authentication method should later be referenced in a client filter, this name should be used.

9. **Enter the Display name for the server.**

   This is an optional field.

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

11. **Click Update.**

    A new authentication ID is created.

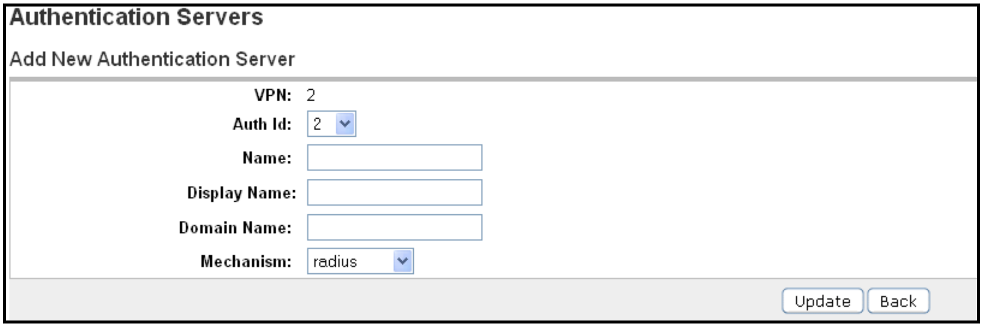
Configure RADIUS Specific Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   The Authentication Server screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

   Add New Authentication server is displayed.



Authentication Servers

Add New Authentication Server

VPN:	2
Auth Id:	2
Name:	
Display Name:	
Domain Name:	
Mechanism:	radius

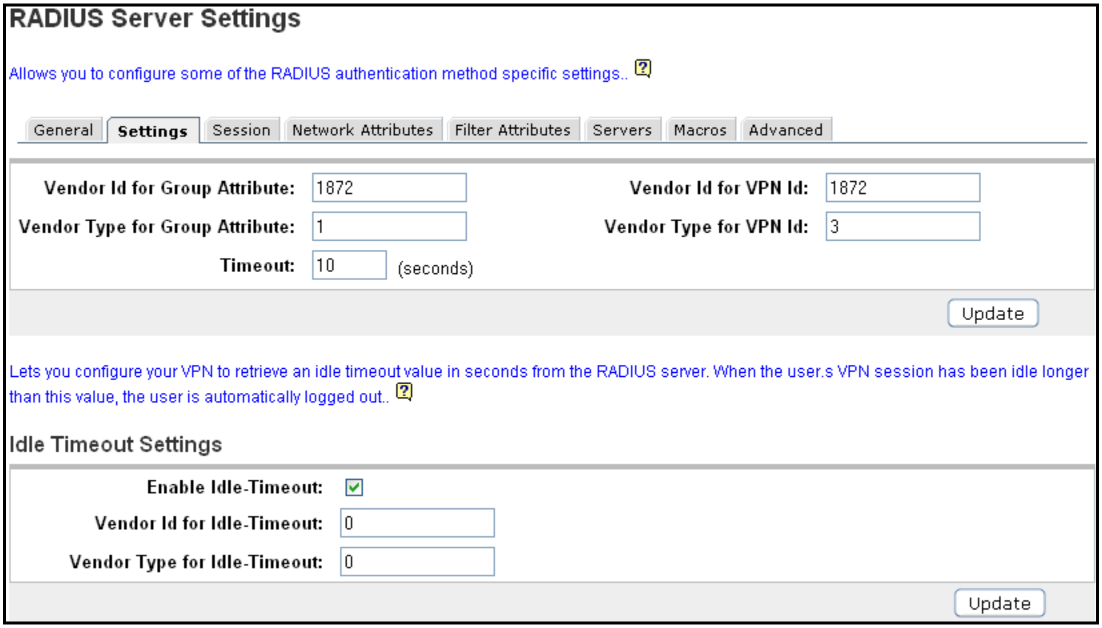
8. **Select the Auth ID.**
9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
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 the Authentication ID in the Authentication Server screen.**

14. **Click the Settings tab.**



RADIUS Server Settings

Allows you to configure some of the RADIUS authentication method specific settings..

Vendor Id for Group Attribute:	1872	Vendor Id for VPN Id:	1872
Vendor Type for Group Attribute:	1	Vendor Type for VPN Id:	3
Timeout:	10 (seconds)		

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..

Idle Timeout Settings

Enable Idle-Timeout:	☑
Vendor Id for Idle-Timeout:	0
Vendor Type for Idle-Timeout:	0

15. **In the Vendor Id field, enter the Vendor-ID for the group attribute.**

    This attribute is set to `1872 (alteon)` by default. It should correspond to the Vendor-Id used by your RADIUS server to send group names to the client. If your RADIUS server uses another Vendor-Id, you can change this value.

    Contact your RADIUS server administrator for more information. If you want to use a standard RADIUS attribute other than vendor-specific, set Vendor-Id to 0 and Vendor Type to the desired attribute number (for example 25 for class).

16. **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.

17. **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 Avaya VPN Gateway), the Avaya VPN Gateway 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.

18. **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 number, the Vendor-Type number identifies the VPN to which the remote user has logged in.

19. **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.

20. **Click Update.**

21. **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.

22. **Click Update.**

Add RADIUS Server

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 system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

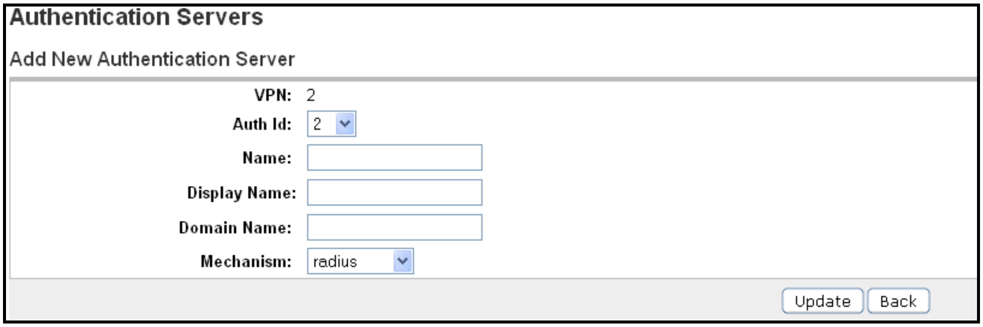
4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present, go to Step 13.**

7. **Click Add.**

   Add New Authentication server is displayed.



Authentication Servers

Add New Authentication Server

VPN:	2
Auth Id:	2
Name:	
Display Name:	
Domain Name:	
Mechanism:	radius

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

11. **Select radius from the Mechanism list.**

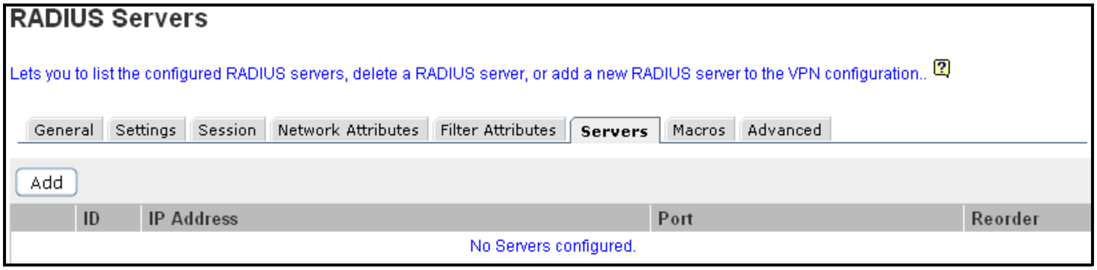
12. **Click Update.**

    A new authentication ID is created.

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

14. **Click the Servers tab and then click Add.**

RADIUS servers is displayed.



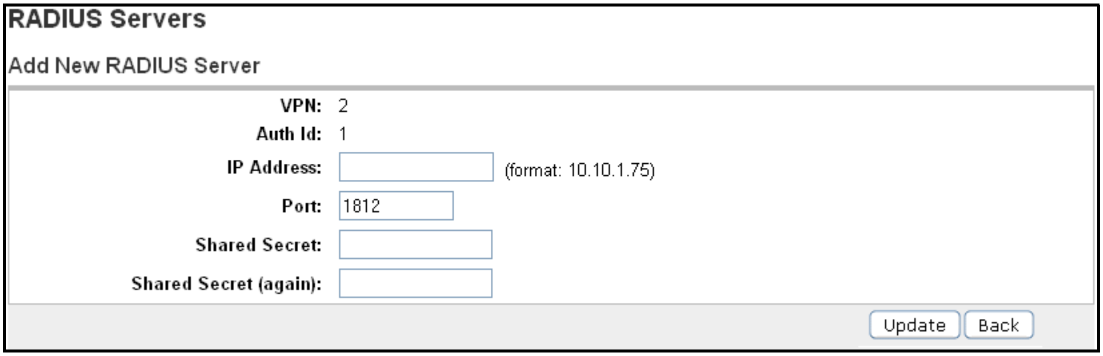
RADIUS Servers

Lets you to list the configured RADIUS servers, delete a RADIUS server, or add a new RADIUS server to the VPN configuration..

	ID	IP Address	Port	Reorder
No Servers configured.				

15. **Click Add.**

    Add new RADIUS Server form is displayed.



RADIUS Servers

Add New RADIUS Server

VPN: 2

Auth Id: 1

IP Address: (format: 10.10.1.75)

Port: 1812

Shared Secret:

Shared Secret (again):

16. **In the IP address field, enter the IP address of the RADIUS server.**
17. **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.
18. **In the Shared Secret fields, enter a unique shared secret (password).**

    The shared secret is used to authenticate the Avaya VPN Gateway to the RADIUS server. Contact your RADIUS server administrator to obtain the shared secret.
19. **Click Update.**
20. **Apply the changes.**

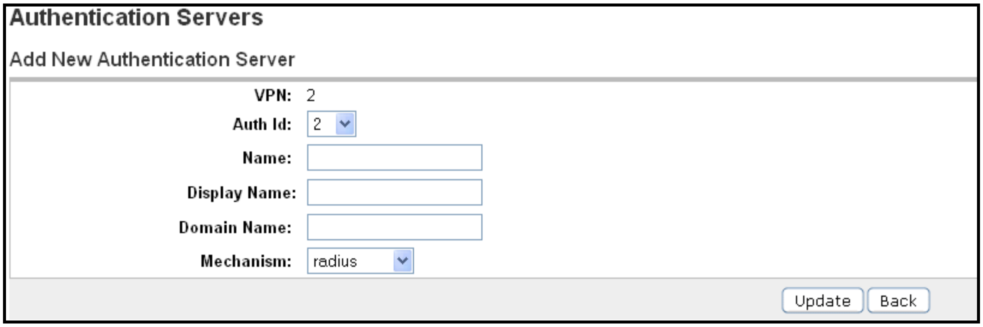
Configure Network Attributes

For Net Direct and Avaya VPN Client connections, client IP address and network attributes can be retrieved from a RADIUS server. This requires that the VPN includes at least one IP pool whose pool mechanism is set to `radius`. How to configure the IP pool is described in Chapter 7, "Net Direct" and Chapter 21, "Transparent Mode", respectively. These chapters also describe how to create a local IP pool on the Avaya VPN Gateway as fallback, if the RADIUS server does not return a specific network attribute.

Specify the required Vendor-Id and Vendor-Type values to retrieve network attributes from the RADIUS server.

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Servers screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

   Add New Authentication server is displayed.



Authentication Servers

Add New Authentication Server

VPN: 2
Auth Id: 2
Name:
Display Name:
Domain Name:
Mechanism: radius

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

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

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

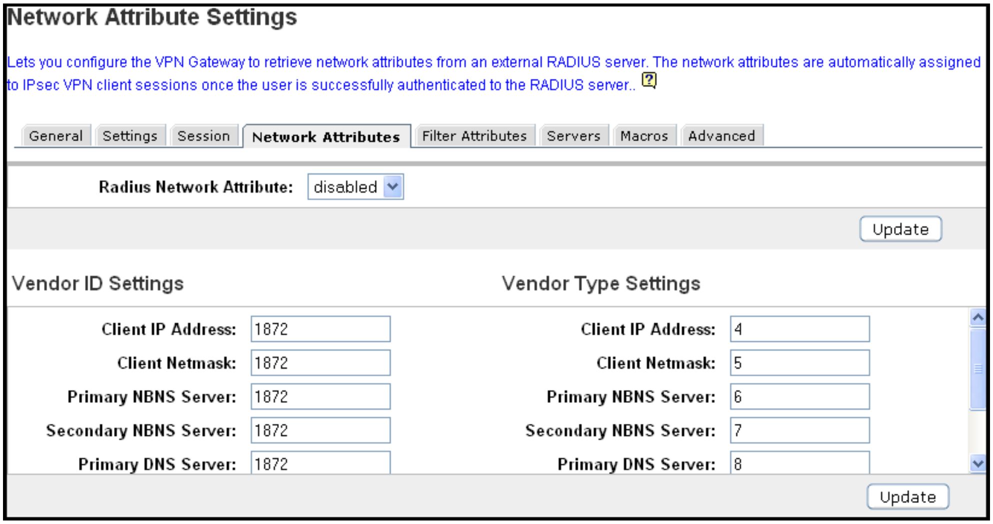
12. **Click Update.**

    A new authentication ID is created.

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

14. **Click the Network Attributes tab.**

    Network Attributes Settings screen is displayed.



Network Attribute Settings

Lets you configure the VPN Gateway to retrieve network attributes from an external RADIUS server. The network attributes are automatically assigned to IPsec VPN client sessions once the user is successfully authenticated to the RADIUS server..

Radius Network Attribute: disabled

Vendor ID Settings		Vendor Type Settings	
Client IP Address:	1872	Client IP Address:	4
Client Netmask:	1872	Client Netmask:	5
Primary NBNS Server:	1872	Primary NBNS Server:	6
Secondary NBNS Server:	1872	Secondary NBNS Server:	7
Primary DNS Server:	1872	Primary DNS Server:	8

15. **Under Vendor ID Settings and Vendor Type Settings, enter the desired settings.**

    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.

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

17. **Configure the Filter Attribute Settings.**

    These steps lets you configure VPN Gateway to retrieve filter attributes from an external RADIUS server.

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server is displayed

8. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

9. **Enter the Display name for the server.**

   This is an optional field.Enable/Disable Radius Filter Attribute.

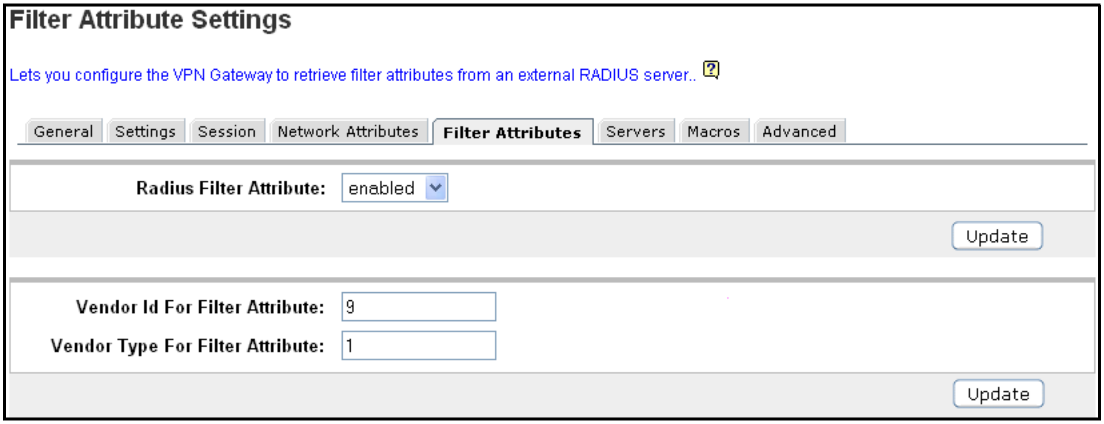
10. **Select radius in Mechanism drop-down list.**

11. **Click Update.**

    A new authentication ID is created.

12. **Click the Authentication ID in the Authentication Server screen.**

13. **Click the Filter Attributes tab.**



Filter Attribute Settings

Lets you configure the VPN Gateway to retrieve filter attributes from an external RADIUS server..

Radius Filter Attribute: enabled

Vendor Id For Filter Attribute: 9

Vendor Type For Filter Attribute: 1

14. **Enable/Disable Radius Filter Attribute.**

15. **Click Update to update the filter status.**

16. **Specify the Vendor Id for the RADIUS Filter attribute.**

17. **Specify the Vendor Type for the RADIUS Filter attribute.**

18. **Click Update to update the specified Filter Attributes.**

Configure RADIUS Session Timeout

These steps (optional) lets you configure your VPN to retrieve a session timeout 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 system administrator.**

2. **Click the Config tab.**

3. **In the System tree view, select VPN Gateways.**

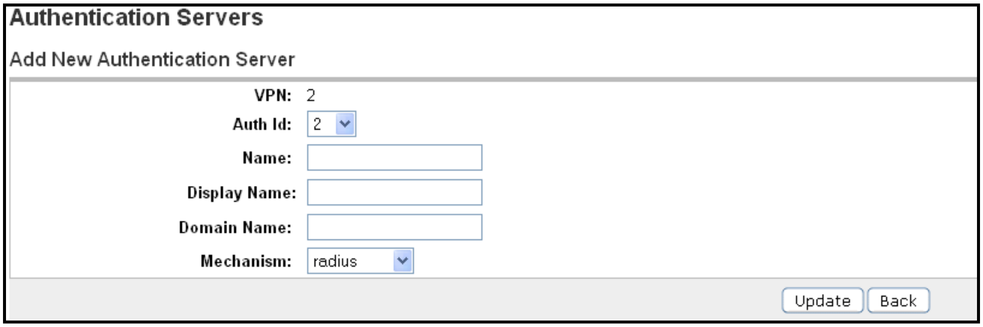
4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Servers screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server is displayed.



Authentication Servers

Add New Authentication Server

VPN: 2

Auth Id: 2

Name:

Display Name:

Domain Name:

Mechanism: radius

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

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

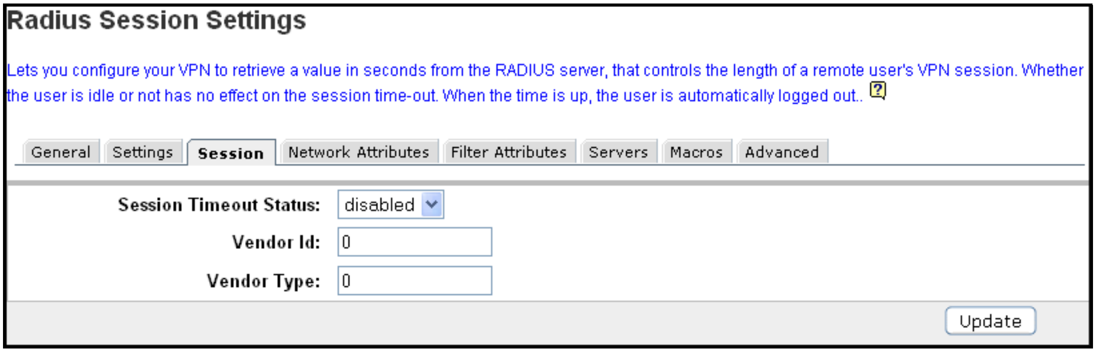
12. **Click Update.**

    A new authentication ID is created.

13. **Click the Authentication ID in Authentication Servers screen.**

14. **Click the Session tab.**

    RADIUS Session screen is displayed.



Radius Session Settings

Lets you configure your VPN to retrieve a value in seconds from the RADIUS server, that 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..

Session Timeout Status: disabled

Vendor Id: 0

Vendor Type: 0

15. **In the Session Timeout Status 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 Exchange Server) to a RADIUS user attribute identifying an Exchange server. Create an Internal Website link and specify the variable in the link properties, e.g. `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 system administrator.**

2. **Click the Config tab.**

3. **In the System tree view, select VPN Gateways.**

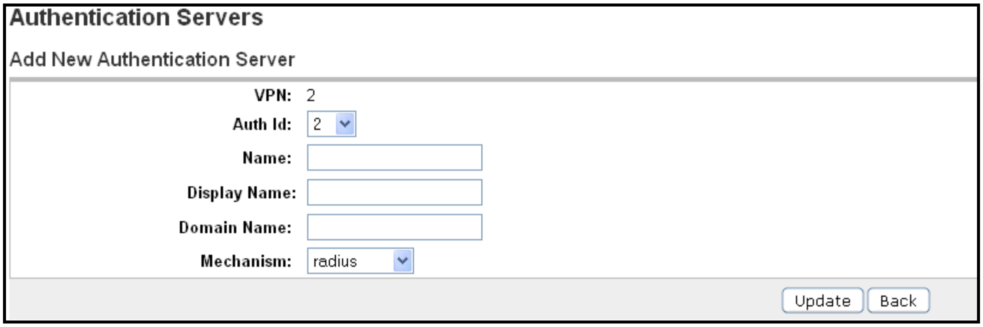
4. **Select the VPN Gateway name for configuring the authentication.**

   Under settings, select Authentication.
   Authentication Servers screen is displayed.

5. **If the Authentication server is already present go to Step 12.**

6. **Click Add.**

   Add New Authentication server is displayed.



Authentication Servers

Add New Authentication Server

VPN:	2
Auth Id:	2
Name:	
Display Name:	
Domain Name:	
Mechanism:	radius

7. **Select the Auth ID.**

8. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

9. **Enter the Display name for the server.**

   This is an optional field.

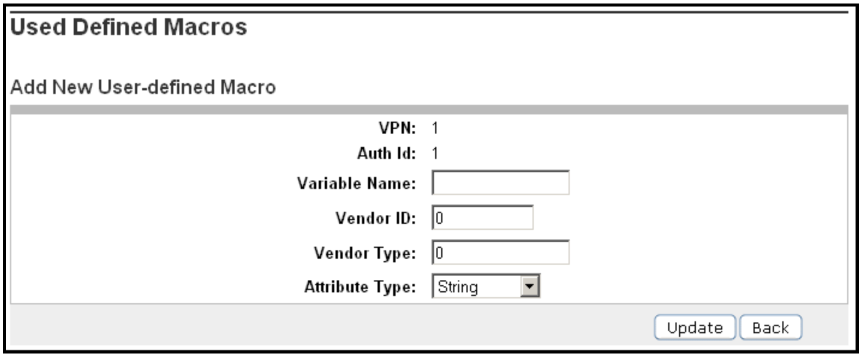
10. **Select radius from the Mechanism list.**

11. **Click Update.**

    A new authentication ID is created.

12. **Click the Authentication ID in Authentication Server screen.**

13. **Click the Macros tab and then click Add.**



Used Defined Macros

Add New User-defined Macro

VPN:	1
Auth Id:	1
Variable Name:	
Vendor ID:	0
Vendor Type:	0
Attribute Type:	String

14. **In the Variable Name field, enter a name of your own choice,** for example `Exchang-eServer`.

    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.

15. **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.

16. **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.

17. **In the Attribute Type list box, select the type of value to be retrieved.**

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

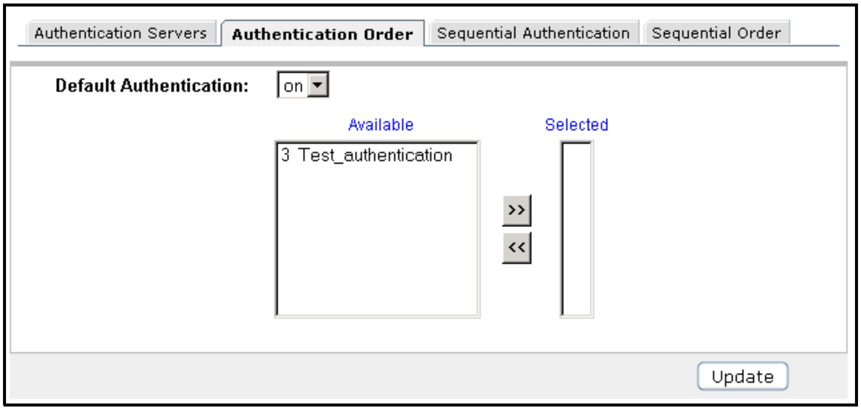
Specify the Authentication Fallback Order

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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
6. **Click the Authentication Order tab.**

   The AuthOrder form is displayed.



Default Authentication: on

Available: 3 Test_authentication

Selected:

7. **From the Default Authentication list, select on to enable the default logon.**
   The Login Service list appears in the Portal logon page.

   Or

   Select off to disable the default logon.
   The configured authentication methods in the authentication order appear in the logon page. The authentication methods must contain a display name when the Default Authentication is off.

8. **Under Fallback Order, in the Available list, select `3 Test_authentication`.**

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 Avaya VPN Gateway ignores the other specified authentication methods (if any) in the Authentication Order list.

Configure Sequential Authentication

Sequential Authentication provides enhanced security by prompting dual authentication credentials to gain access to the portal. The portal presents two distinct logon pages for authenticating two authentication servers sequentially. After successful authentication of the primary authentication server, the second logon screen appears for Secondary Authentication. If the Secondary Authentication fails, retries are allowed before switching back to the primary logon screen. Secondary Authentication is for each VPN setting. The Secondary Authentication is limited to portal users, and is not supported for IPSec and Net Direct installed client users.

IPSec Two Factor authentication method provides support for IPSec and Net Direct 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. With this option you can enable both SSL Secondary Authentication and IPsec Two Factor authentication.

When configuring certificate authentication, IPsec Two Factor Authentication adds more security than SSL Secondary Authentication by requiring that the client provide 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.

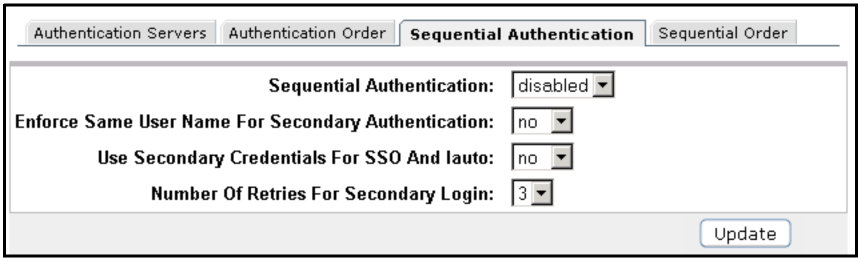
To configure Sequential Authentication, perform the following:

1. **Log on to the BBI as administrator.**
2. **Select Config.**
3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.
5. **Select Authentication.**
6. **Select Sequential Authentication.**

   The Sequential Authentication Order form appears.



Sequential Authentication: disabled
Enforce Same User Name For Secondary Authentication: no
Use Secondary Credentials For SSO And Iauto: no
Number Of Retries For Secondary Login: 3

7. **From the Sequential Authentication list, select enabled.**
8. **From the Enforce Same User Name For Secondary Authentication list, select yes to automatically update the user name field in the secondary logon page with the primary authentication user name.**
   You cannot change the user name field value.

   Or

   Select no, to enter the user name field in the secondary logon page.
9. **From the Use Secondary Credentials For SSO And Iauto list, select yes.**
10. **From the Number Of Retries For Secondary Login list, select the number of retries.**
11. **Click Update.**

12. **Click Apply.**

Specify Authentication Order

Sequential Authentication Order is applicable when you enable Sequential Authentication. Authentication Order sets the preferred order for which the defined authentication methods are applied when a remote user logs on using the secondary logon page into the Portal.

To configure Authentication Order, perform the following steps:

1. **Log on to the BBI as administrator.**

2. **Select Config.**

3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

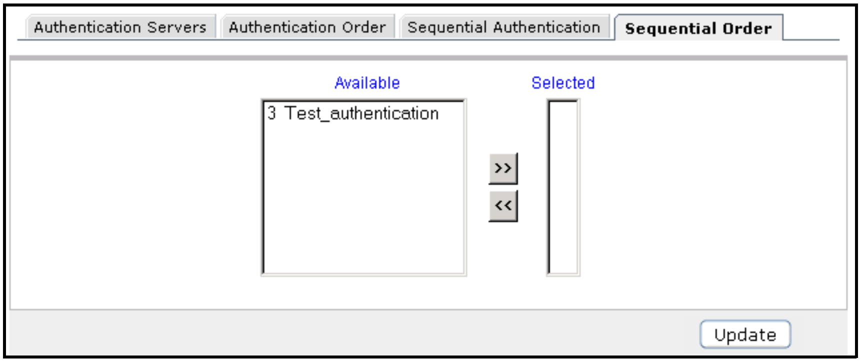
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**

6. **Select Sequential Order.**

   The Sequential Order form appears.



3 Test_authentication

7. **From the Available list, select `3 Test_authentication.`**

8. **Click >> to move the item to the Selected list.**

9. **Click Update.**

10. **Apply changes.**

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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**

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

   Add New Authentication server is displayed.
7. **Select the Auth ID.**
8. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
9. **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 Avaya VPN Client 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.
10. **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 Chapter 11, “Group Links”.

11. **Select LDAP from the Mechanism list.**

    Add New LDAP Server screen is displayed.

12. **Click Resolve IP.**

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

13. **Specify the iSD Bind Password and enable LDAPS.**

14. **Click Update.**

Configure LDAP Specific Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Servers screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server form is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

11. **Select ldap from the Mechanism list.**

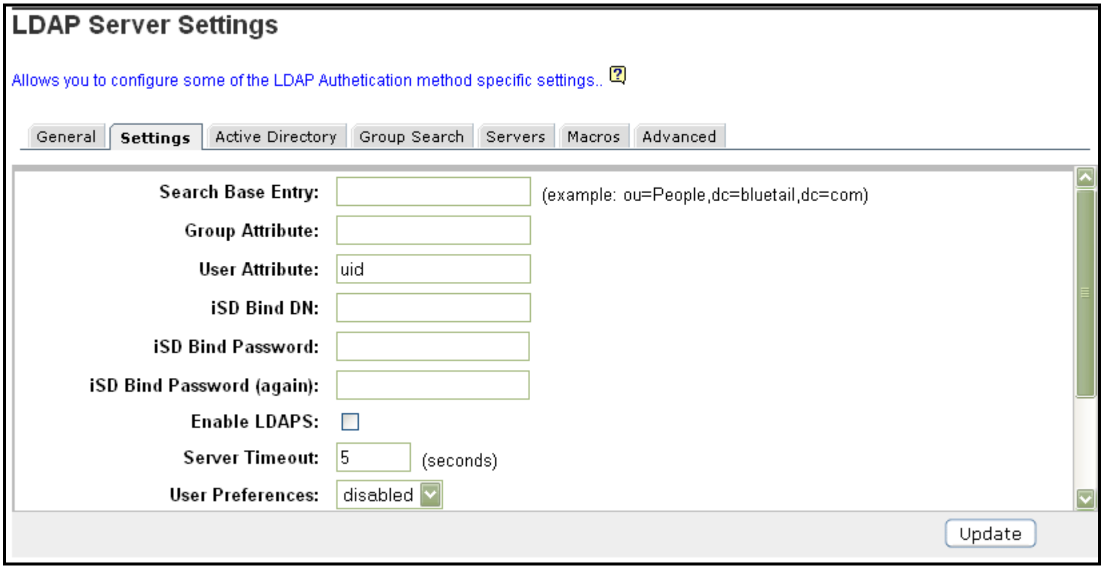
12. **Click Update.**

    A new authentication ID is created.

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

14. **Click the Settings tab.**

    The LDAP Server Settings form appears.



LDAP Server Settings

Allows you to configure some of the LDAP Authetication method specific settings..

Search Base Entry:		(example: ou=People,dc=bluetail,dc=com)
Group Attribute:		
User Attribute:	uid	
iSD Bind DN:		
iSD Bind Password:		
iSD Bind Password (again):		
Enable LDAPS:	☐	
Server Timeout:	5	(seconds)
User Preferences:	disabled	

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 Avaya VPN Gateway to authenticate to the LDAP server, using the values specified for `isdBindDN` and `isdBindPassword`. Also see example in the section "Search the LDAP Dictionary Information Tree (DIT)" on page 278.

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 contained in the LDAP attribute must be defined for the VPN on the Avaya 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 Avaya VPN Gateway should authenticate. Normally, this step (and iSD Bind Password) can be skipped. It is only required if the Avaya VPN Gateway should authenticate to the LDAP server, for example to be able to search the Dictionary Information tree (DIT). See the example in section "Search the LDAP Dictionary Information Tree (DIT)" on page 278.

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

    If checked, LDAP requests between the Avaya 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 Avaya 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 Avaya 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 Step 24 and Step 25). 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 if the extra search filter is disabled (see Step 23).

    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 if the extra search filter is disabled (see Step 23).

    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 Avaya VPN Gateway 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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication. If the Authentication server is already present go to Step 13.**

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

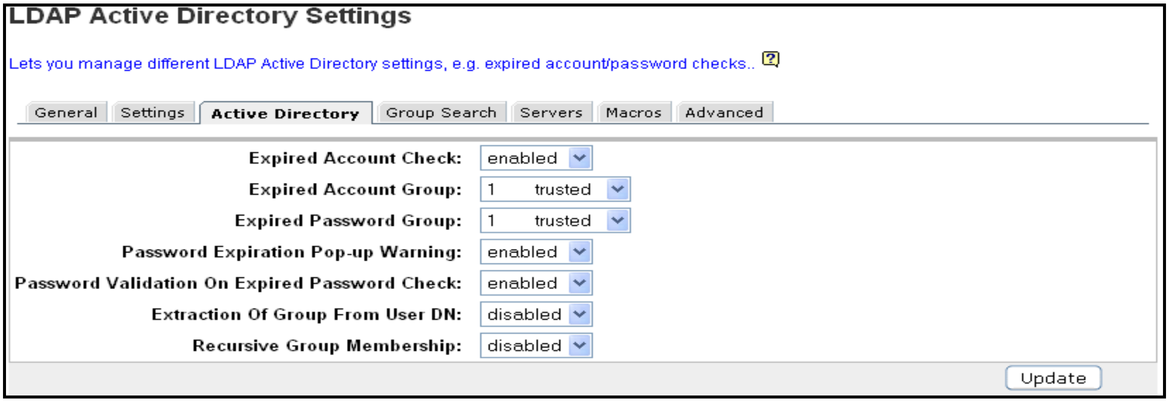
   Add New Authentication server form is displayed.
7. **Select the Auth ID.**
8. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing authentication method.
9. **Enter the Display name for the server.**

   This is an optional field.
10. **Select ldap from the Mechanism list.**
11. **Click Update.**

    A new authentication ID is created.
12. **Click on the Authentication ID in Authentication Server screen.**
13. **Click on Active Directory tab.**

The LDAP Active Directory Settings form is displayed.



LDAP Active Directory Settings

Lets you manage different LDAP Active Directory settings, e.g. expired account/password checks..

Expired Account Check:	enabled
Expired Account Group:	1 trusted
Expired Password Group:	1 trusted
Password Expiration Pop-up Warning:	enabled
Password Validation On Expired Password Check:	enabled
Extraction Of Group From User DN:	disabled
Recursive Group Membership:	disabled

14. **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.

    First, create a user access group on the Avaya 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 Chapter 8, “Groups, Access Rules and Profiles.

15. **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.

16. **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.

17. **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.**

18. **Specify whether to enable/disable password validation on expired password check.**

19. **Enable/Disable extraction of group from user DN if the Active Directory does not return any group for a user.**

20. **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.

21. **Click Update.**

Configure Group Search Settings

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

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server form is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

10. **Enter the Display name for the server.**

This is an optional field.

11. **Select ldap from the Mechanism list.**

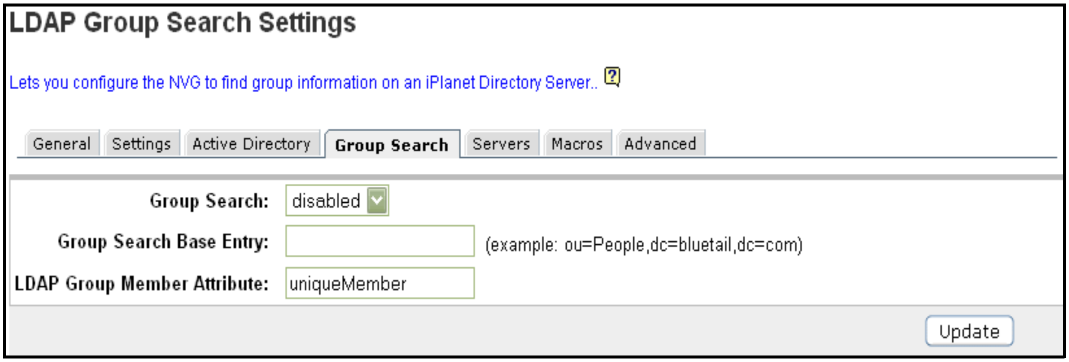
12. **Click Update.**

    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 is displayed.



LDAP Group Search Settings

Lets you configure the NVG to find group information on an iPlanet Directory Server..

Group Search: disabled

Group Search Base Entry: (example: ou=People,dc=bluetail,dc=com)

LDAP Group Member Attribute: uniqueMember

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 page 264). Using the preceding example, the group name `Staff` would 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 system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present, go to Step 13**

7. **Click Add.**

   Add New Authentication server is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

10. **Enter the Display name for the server.**

    This is an optional field.

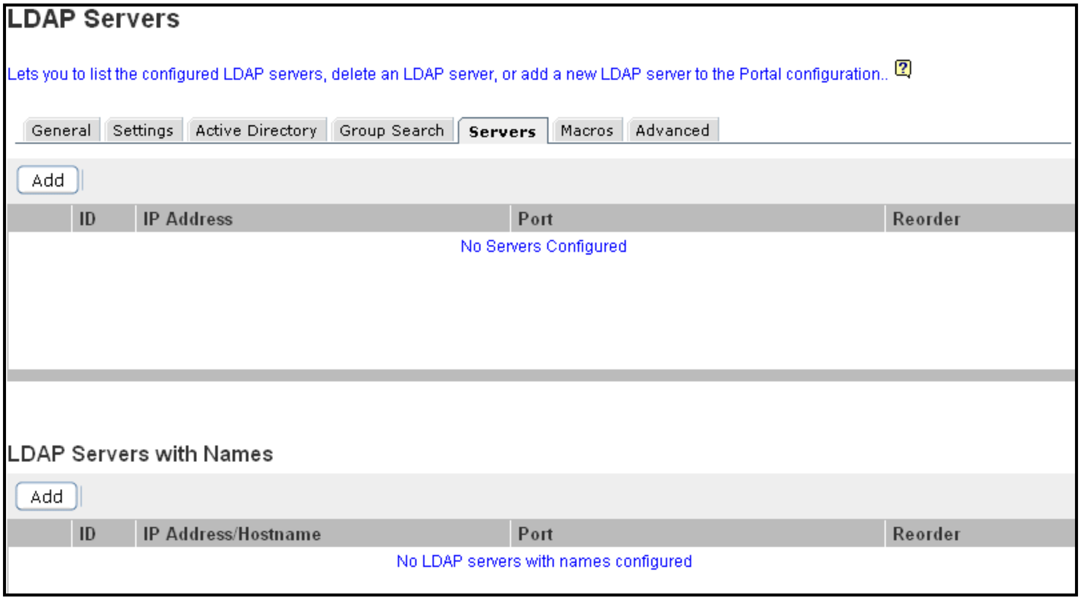
11. **Select ldap from the Mechanism list.**

12. **Click Update.**

    A new authentication ID is created.

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

14. **Click on Servers tab. The LDAP Servers form is displayed.**



LDAP Servers

Lets you to list the configured LDAP servers, delete an LDAP server, or add a new LDAP server to the Portal configuration..

	ID	IP Address	Port	Reorder

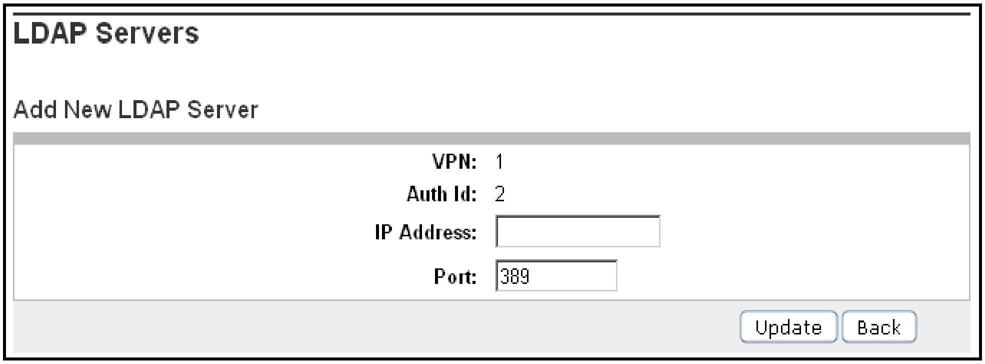
No Servers Configured

LDAP Servers with Names

	ID	IP Address/Hostname	Port	Reorder

No LDAP servers with names configured

15. **Click Add in LDAP sever table.**



LDAP Servers

Add New LDAP Server

VPN: 1

Auth Id: 2

IP Address:

Port: 389

16. **In the IP Address field, enter the IP address for the LDAP server.**

17. **In the Port field, enter the port number you want to use.**

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 Avaya VPN Gateway and the LDAP server, port number 636 should be used.

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

LDAP Server with names

You can specify the fully qualified domain name of the LDAP server by using LDAP Servers with Names. To add a LDAP server with names follow these steps:

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**

   Under settings, select Authentication.
   Authentication Server screen is displayed.

5. **If the Authentication server is already present, go to Step 13.**
6. **Click Add.**

   Add New Authentication server is displayed.

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

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

9. **Enter the Display name for the server.**

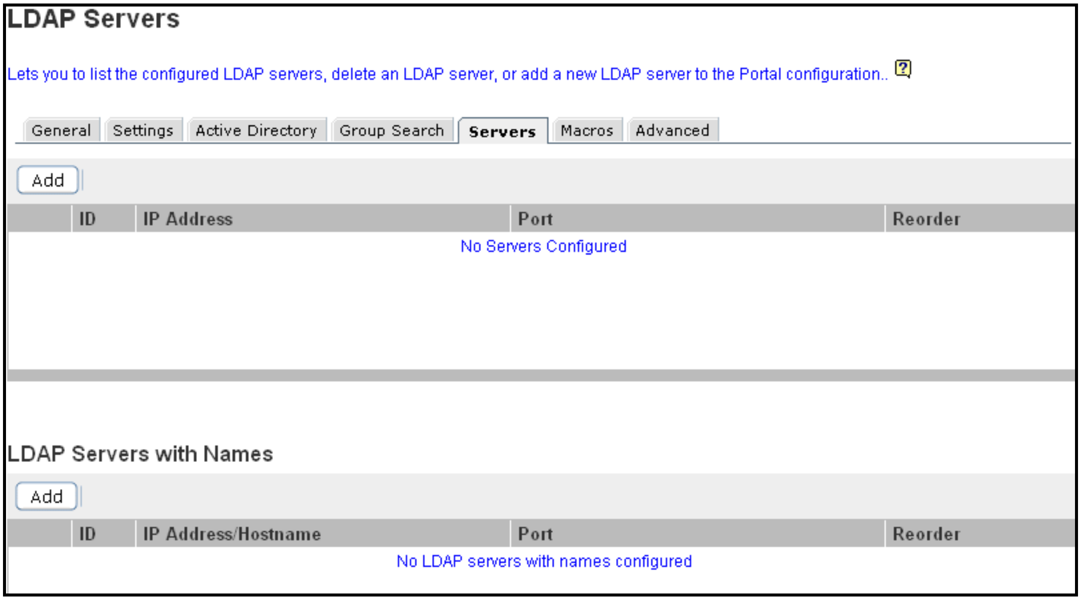
   This is an optional field.

10. **Select ldap from the Mechanism list.**
11. **Click Update.**

    A new authentication ID is created.

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

13. **Click on Servers tab. The LDAP Servers form is displayed.**



LDAP Servers

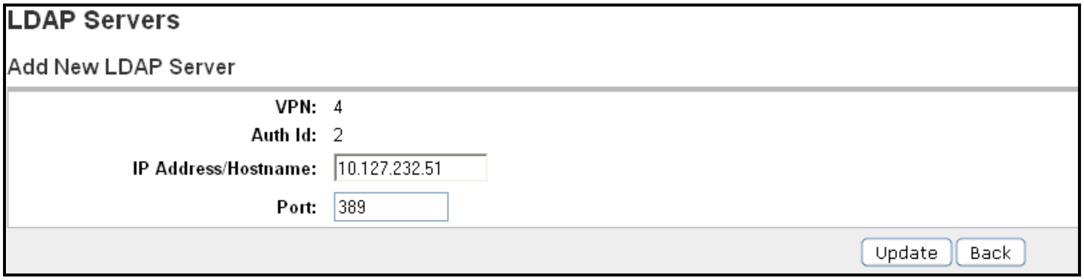
Lets you to list the configured LDAP servers, delete an LDAP server, or add a new LDAP server to the Portal configuration..

ID	IP Address	Port	Reorder
No Servers Configured			

LDAP Servers with Names

ID	IP Address/Hostname	Port	Reorder
No LDAP servers with names configured			

14. **Click Add in LDAP Servers with Names table.**



LDAP Servers

Add New LDAP Server

VPN: 4
Auth Id: 2
IP Address/Hostname: 10.127.232.51
Port: 389

15. **Specify the IP address or fully qualified domain name of LDAP server. This option is available when you add or edit an LDAP server using the LDAP Servers with Names table.**

16. **Specify TCP port number.**

The Port must be a positive integer less than or equal to 65535.

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, e.g. `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 system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

10. **Enter the Display name for the server.**

    This is an optional field.

11. **Select ldap from the Mechanism list.**

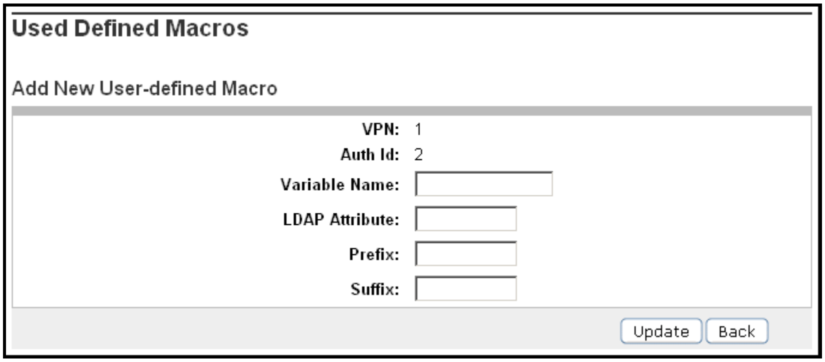
12. **Click Update.**

    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 is displayed.



Used Defined Macros

Add New User-defined Macro

VPN:	1
Auth Id:	2
Variable Name:	
LDAP Attribute:	
Prefix:	
Suffix:	

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.**

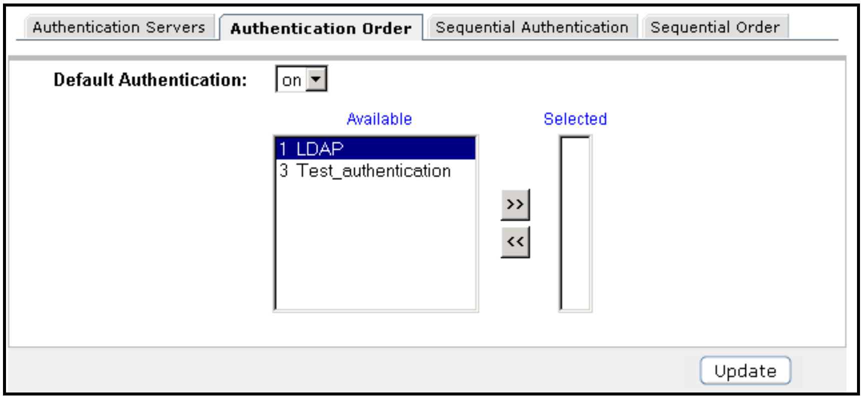
Specify the Authentication Fallback Order

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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
6. **Click the Authentication Order tab.**

   The Authentication Order form appears.



Default Authentication: on

1 LDAP
3 Test_authentication

7. **From the Default Authentication list, select on to enable the default logon.**
   The Login Service list appears in the Portal login page.

   Or

   Select off to disable the default logon.
   The configured authentication methods in the authentication order appears in the logon page. The authentication methods must contain a display name when the Default Authentication is off.
8. **Under Fallback Order, in the Available list, select `1 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 Avaya VPN Gateway ignores the other specified authentication methods (if any) in the Authentication Order list.

Configure Sequential Authentication

Sequential Authentication provides enhanced security by prompting dual authentication credentials to gain access to the portal. The portal presents two distinct logon pages for authenticating two authentication servers sequentially. After successful authentication of the primary authentication server, the second logon screen appears for Secondary Authentication. If the Secondary Authentication fails, retries are allowed before switching back to the primary logon screen. Secondary Authentication is for each VPN setting. The Secondary Authentication is limited to portal users, and is not supported for IPSec and Net Direct installed client users.

IPSec Two Factor authentication method provides support for IPSec and Net Direct 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. With this option you can enable both SSL Secondary Authentication and IPsec Two Factor authentication.

When configuring certificate authentication, IPsec Two Factor Authentication adds more security than SSL Secondary Authentication by requiring that the client provide 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.

To configure Sequential Authentication, perform the following:

1. **Log on to the BBI as administrator.**

2. **Select Config.**

3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

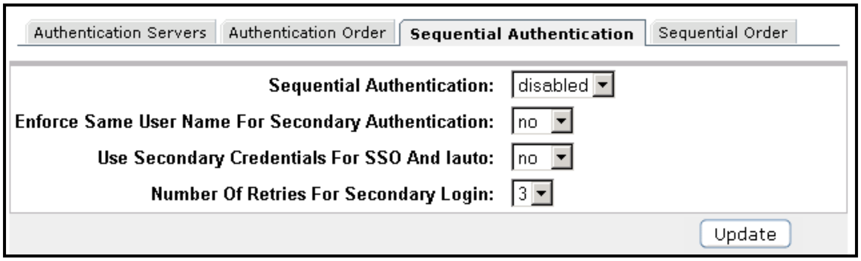
4. **Select the configured VPN for which you want to enable authentication.**

The VPN Summary form appears.

5. **Select Authentication.**

6. **Select Sequential Authentication.**

   The Sequential Authentication Order form appears.



Sequential Authentication: disabled

Enforce Same User Name For Secondary Authentication: no

Use Secondary Credentials For SSO And Iauto: no

Number Of Retries For Secondary Login: 3

7. **From the Sequential Authentication list, select enabled.**

8. **From the Enforce Same User Name For Secondary Authentication list, select yes to automatically update the user name field in the secondary logon page with the primary authentication user name.**
   You cannot change the user name field value.

   Or

   Select no, to enter the user name field in the secondary logon page.

9. **From the Use Secondary Credentials For SSO And Iauto list, select yes.**

10. **From the Number Of Retries For Secondary Login list, select the number of retries.**

11. **Click Update.**

12. **Click Apply.**

Specify Authentication Order

Sequential Authentication Order is applicable when you enable Sequential Authentication. Authentication Order sets the preferred order for which the defined authentication methods are applied when a remote user logs on using the secondary logon page into the Portal.

To configure Authentication Order, perform the following:

1. **Log on to the BBI as administrator.**

2. **Select Config.**

3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

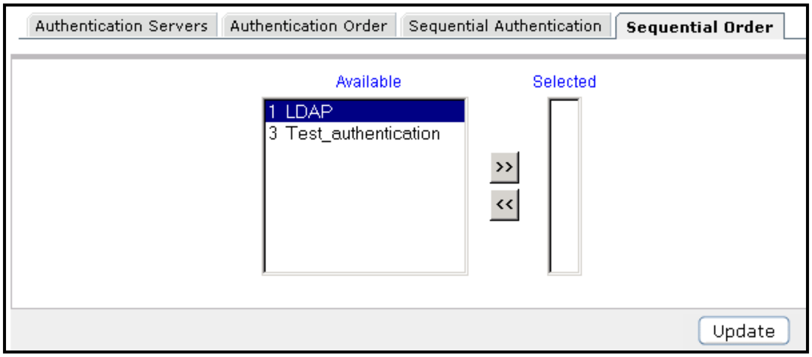
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**

6. **Select Sequential Order.**

   The Sequential Order form appears.



7. **From the Available list, select `1 LDAP`.**

8. **Click >> to move the item to the Selected list.**

9. **Click Update.**

10. **Apply changes.**

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 system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server form is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

10. **Enter the Display name for the server.**

    This is an optional field.

11. **Select ldap from the Mechanism list.**

12. **Click Update.**

    A new authentication ID is created.

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

14. **Click the 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 Avaya VPN Gateway authentication.**

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

18. **In the iSD Bind Password field, set a password for Avaya VPN Gateway authentication.**

    This step sets the password to be used when the Avaya 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 260).

Configure Basic Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

   Authentication Server screen is displayed.

6. **Click Add.**

   Add New Authentication server is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter a name for the authentication method for example `ntlm`.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later. For more information about client filters, see Chapter 8, “Groups, Access Rules and Profiles”.

9. **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, in the Avaya VPN Client 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.

   By selecting `default` from the Logon Service list on the Portal logon page, authentication is carried out according to the configured authentication order.

10. **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 Chapter 11, “Group Links”.

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

12. **Click Update.**

NTLM Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication. If the Authentication server is already present go to Step 12.**

   Authentication Server screen is displayed.

6. **Click Add.**

Add New Authentication server form is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

9. **Enter the Display name for the server.**

   This is an optional field.

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

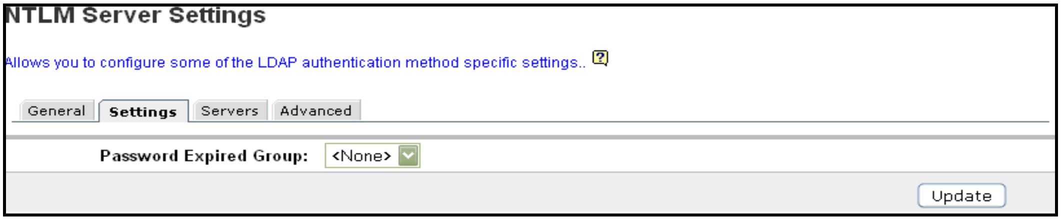
11. **Click Update.**

    A new authentication ID is created.

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

13. **Click the Settings tab.**

    The NTLM Server Settings form appears.



NTLM Server Settings

Allows you to configure some of the LDAP authentication method specific settings..

Password Expired Group: <None>

14. **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 Avaya VPN Gateway. 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.

15. **Click Update.**

Add NTLM Server(s)

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

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present, go to Step 13**

7. **Click Add.**

   Add New Authentication server is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

10. **Enter the Display name for the server.**

    This is an optional field.

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

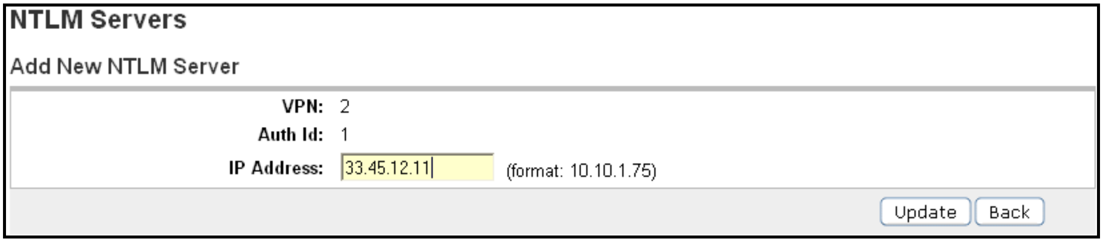
12. **Click Update.**

    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 NTLM Server form is displayed.



NTLM Servers

Add New NTLM Server

VPN:	2
Auth Id:	1
IP Address:	33.45.12.11 (format: 10.10.1.75)

15. **In the IP address field, enter the IP address of the NTLM server.**

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

Configure Advance NTLM Settings

This section enables you to configure advanced settings of NTLM authentication.

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present, go to Step 13**

7. **Click Add.**

   Add New Authentication server is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later.

10. **Enter the Display name for the server.**

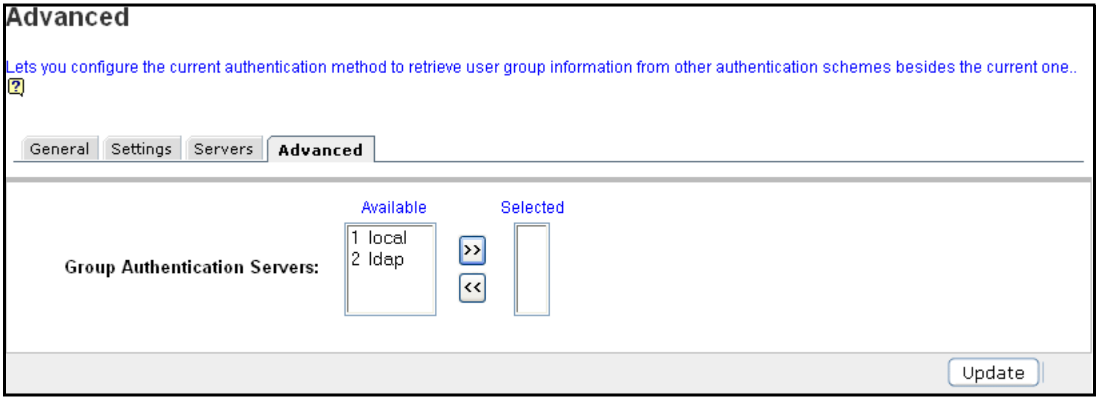
    This is an optional field.

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

12. **Click Update.**

    A new authentication ID is created.

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



Advanced

Lets you configure the current authentication method to retrieve user group information from other authentication schemes besides the current one..

Group Authentication Servers:

Available: 1 local, 2 ldap

Selected:

14. **Click on Advance tab.**

    By referencing a previously defined authentication server here, the system retrieves the SSL VPN user's group information from the corresponding authentication scheme.

    Example: The user logs in via RADIUS but the user groups are stored in an LDAP database. By selecting the list of authentication servers, the system checks each corresponding authentication scheme to see if the user name can be matched against user groups defined in these authentication databases. All user groups found in the referenced authentication scheme(s) will be maintained during the SSL VPN user's login session.

15. **Click Update.**

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 system administrator.**

2. **Click on Config tab.**

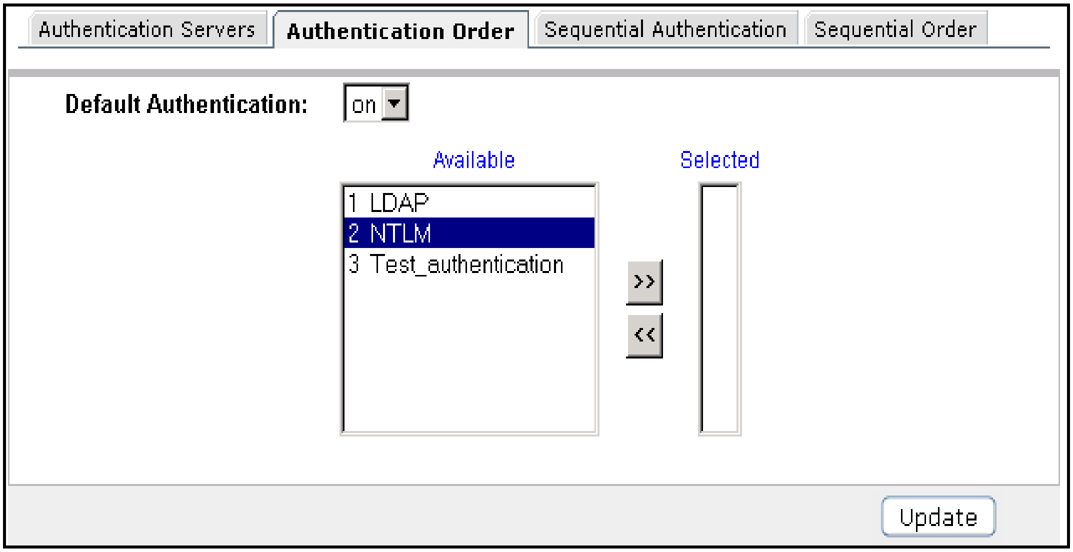
3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

6. **Click the Authentication Order tab.**

   The Authentication Order form appears.



Default Authentication: on

Available	Selected
1 LDAP 2 NTLM 3 Test_authentication	

7. **From the Default Authentication list, select on to enable the default logon.**
   The Login Service list appears in the Portal logon page.

   Or

   Select off to disable the default logon.
   The configured authentication methods in the authentication order appears in the logon page. The authentication methods must contain a display name when the Default Authentication is off.

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 Avaya VPN Gateway ignores the other specified authentication methods (if any) in the Authentication Order list.

Configure Sequential Authentication

Sequential Authentication provides enhanced security by prompting dual authentication credentials to gain access to the portal. The portal presents two distinct logon pages for authenticating two authentication servers sequentially. After successful authentication of the primary authentication server, the second login screen appears for Secondary Authentication. If the Secondary Authentication fails, retries are allowed before switching back to the primary logon screen. Secondary Authentication is for each VPN setting. The Secondary Authentication is limited to portal users, and is not supported for IPSec and Net Direct installed client users.

IPSec Two Factor authentication method provides support for IPSec and Net Direct 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. With this option you can enable both SSL Secondary Authentication and IPsec Two Factor authentication.

When configuring certificate authentication, IPsec Two Factor Authentication adds more security than SSL Secondary Authentication by requiring that the client provide 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.

To configure Sequential Authentication, perform the following:

1. **Log on to the BBI as administrator.**

2. **Select Config.**

3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

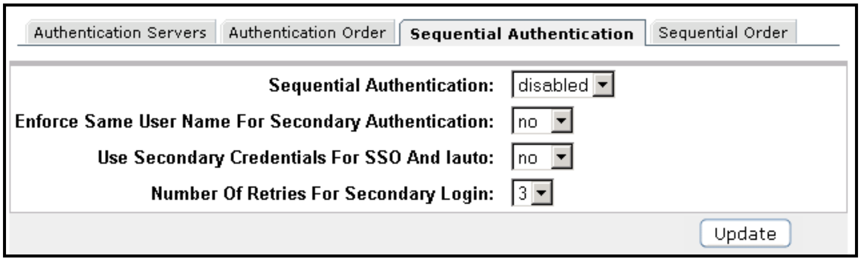
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**

6. **Select Sequential Authentication.**

The Sequential Authentication Order form appears.



Sequential Authentication: disabled

Enforce Same User Name For Secondary Authentication: no

Use Secondary Credentials For SSO And Iauto: no

Number Of Retries For Secondary Login: 3

7. **From the Sequential Authentication list, select enabled.**

8. **From the Enforce Same User Name For Secondary Authentication list, select yes to automatically update the user name field in the secondary logon page with the primary authentication user name.**
   You cannot change the user name field value.

   Or

   Select no, to enter the user name field in the secondary logon page.

9. **From the Use Secondary Credentials For SSO And Iauto list, select yes.**

10. **From the Number Of Retries For Secondary Login list, select the number of retries.**

11. **Click Update.**

12. **Click Apply.**

Specify Authentication Order

Sequential Authentication Order is applicable when you enable Sequential Authentication. Authentication Order sets the preferred order for which the defined authentication methods are applied when a remote user logs on using the secondary logon page into the Portal.

To configure Authentication Order, perform the following:

1. **Log on to the BBI as administrator.**

2. **Select Config.**

3. **From the System tree view, select VPN Gateways.**

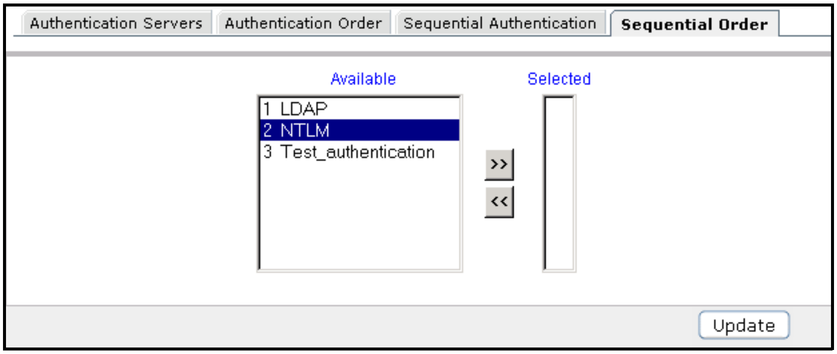
   The VPN Gateways form appears.

4. **Select the configured VPN for which you want to enable authentication.**

The VPN Summary form appears.

5. **Select Authentication.**
6. **Select Sequential Order.**

   The Sequential Order form appears.



7. **From the Available list, select `2 NTLM`.**
8. **Click >> to move the item to the Selected list.**
9. **Click Update.**
10. **Apply changes.**

Netegrity SiteMinder Authentication

To configure the Avaya VPN Gateway 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 Avaya VPN Gateway acts as a client, or agent, to the SiteMinder server. Therefore, the Avaya 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. If not, the Technical Configuration Guide *Using Netegrity SiteMinder with SSL VPN* explains the SiteMinder part of the configuration. It can be found at www.avaya.com. See the latest Release Notes for documentation download instructions.

NOTE – SiteMinder authentication cannot be configured for VPNs that are bound to a specific interface, under VPN Gateways>VPN #>Interface. Binding VPNs to interfaces are typically used in a Secure Service Partitioning configuration (also see Chapter 17, "Secure Service Partitioning"). An exception to the above is when common authentication is enabled for the VPN (under VPN Gateways>VPN #>Interface).

Configure Basic Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

   Authentication Server screen is displayed.

6. **Click Add.**

   Add New Authentication server is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter a name for the authentication method, for example `Site-Minder`.**

   A name is mandatory. Use this authentication server name while referencing the authentication method later. For more information about client filters, see Chapter 8, "Groups, Access Rules and Profiles".

9. **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, in the Avaya VPN Client 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.

   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.

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

This step lets you specify an SiteMinder 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 Chapter 11, “Group Links”.

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

Configure SiteMinder Settings

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

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

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

    This is an optional field.
11. **Select SiteMinder 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 the 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 Avaya 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 Avaya VPN Gateway will connect to the server configured with index number 2.

    The default failover 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 Avaya VPN Gateway.**

    The Avaya 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 Avaya 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 Avaya 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 (e.g. `vpn.example.com`) and the other SiteMinder-enabled site (e.g. `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 Avaya 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 Avaya 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. This field contains the default value GET:/.

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.**

Configure SiteMinder Server(s)

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

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present, go to Step 13.**

7. **Click Add.**

   Add New Authentication server is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

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

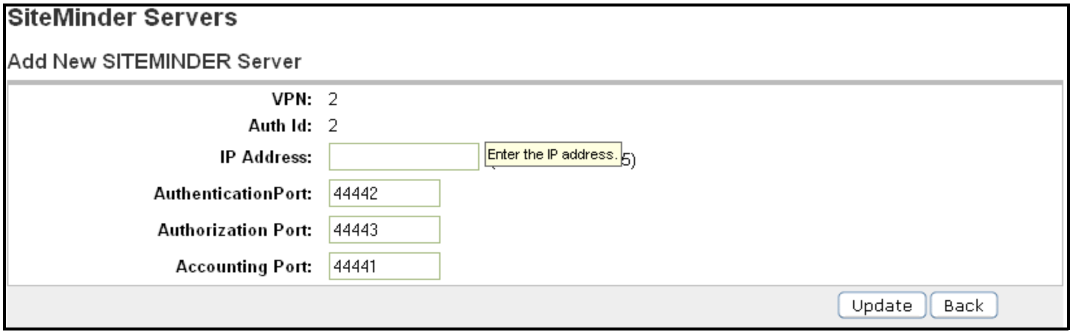
12. **Click Update.**

    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 SiteMinder Server form is displayed.



SiteMinder Servers

Add New SITEMINDER Server

VPN:	2
Auth Id:	2
IP Address:	
AuthenticationPort:	44442
Authorization Port:	44443
Accounting Port:	44441

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.**

Configure Advance SiteMinder Settings

This section enables you to configure advanced settings of SiteMinder authentication.

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present, go to Step 13.**
7. **Click Add.**

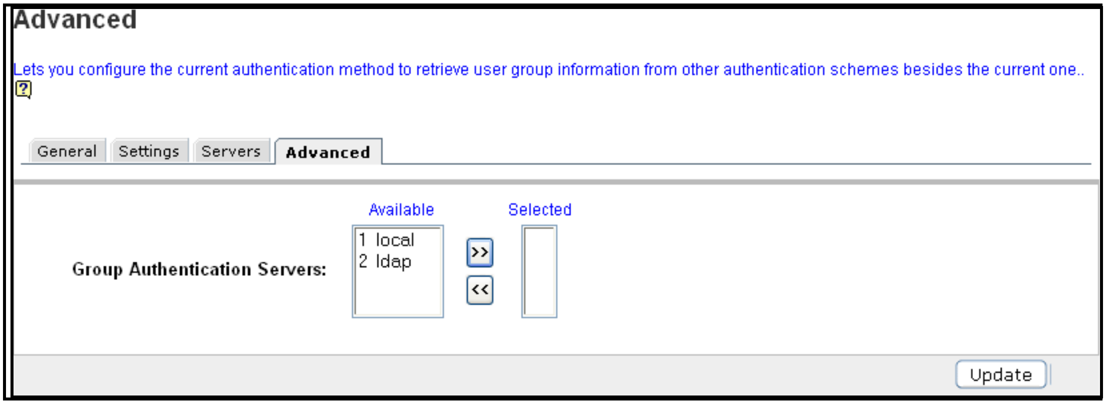
   Add New Authentication server is displayed.
8. **Select the Auth ID.**
9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

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

    A new authentication ID is created.

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



Advanced

Lets you configure the current authentication method to retrieve user group information from other authentication schemes besides the current one..

Group Authentication Servers: Available: 1 local, 2 ldap; Selected: (empty)

14. **Click on Advance tab.**

    By referencing a previously defined authentication server here, the system retrieves the SSL VPN user's group information from the corresponding authentication scheme.

    Example: The user logs in via RADIUS but the user groups are stored in an LDAP database. By selecting the list of authentication servers, the system checks each corresponding authentication scheme to see if the user name can be matched against user groups defined in these authentication databases. All user groups found in the referenced authentication scheme(s) will be maintained during the SSL VPN user's login session.

15. **Click Update.**

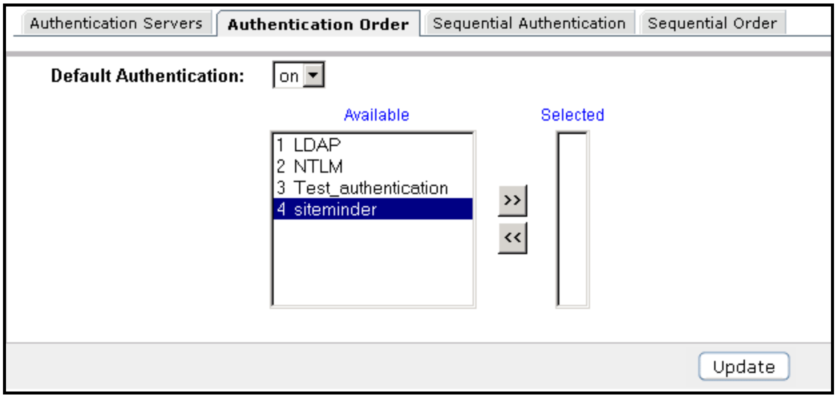
Specify the Authentication Fallback Order

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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
6. **Click the Authentication Order tab.**

   The AuthOrder form is displayed.



Default Authentication: on

Available
1 LDAP
2 NTLM
3 Test_authentication
4 siteminder

Selected

7. **From the Default Authentication list, select on to enable the default logon.**
   The Login Service list appears in the Portal logon page.

   Or

   Select off to disable the default logon.
   The configured authentication methods in the authentication order appear in the logon page. The authentication methods must contain a display name when the Default Authentication is off.

8. **Under the Fallback Order, in the Available list, select `4 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 Avaya VPN Gateway ignores the other specified authentication methods (if any) in the Authentication Order list.

Configure Sequential Authentication

Sequential Authentication provides enhanced security by prompting dual authentication credentials to gain access to the portal. The portal presents two distinct logon pages for authenticating two authentication servers sequentially. After successful authentication of the primary authentication server, the second logon screen appears for Secondary Authentication. If the Secondary Authentication fails, retries are allowed before switching back to the primary logon screen. Secondary Authentication is for each VPN setting. The Secondary Authentication is limited to portal users, and is not supported for IPSec and Net Direct installed client users.

IPSec Two Factor authentication method provides support for IPSec and Net Direct 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. With this option you can enable both SSL Secondary Authentication and IPsec Two Factor authentication.

When configuring certificate authentication, IPsec Two Factor Authentication adds more security than SSL Secondary Authentication by requiring that the client provide 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.

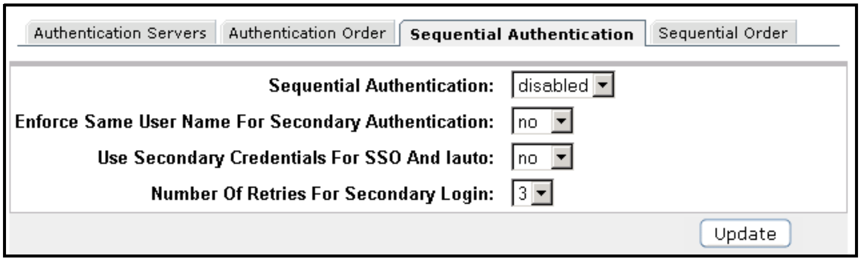
To configure Sequential Authentication, perform the following:

1. **Log on to the BBI as administrator.**
2. **Select Config.**
3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.
5. **Select Authentication.**
6. **Select Sequential Authentication.**

   The Sequential Authentication Order form appears.



Sequential Authentication: disabled

Enforce Same User Name For Secondary Authentication: no

Use Secondary Credentials For SSO And Iauto: no

Number Of Retries For Secondary Login: 3

7. **From the Sequential Authentication list, select enabled.**
8. **From the Enforce Same User Name For Secondary Authentication list, select yes to automatically update the user name field in the secondary logon page with the primary authentication user name.**

   You cannot change the user name field value.

   Or

   Select no, to enter the user name field in the secondary logon page.
9. **From the Use Secondary Credentials For SSO And Iauto list, select yes.**
10. **From the Number Of Retries For Secondary Login list, select the number of retries.**
11. **Click Update.**

12. **Click Apply.**

Specify Authentication Order

Sequential Authentication Order is applicable when you enable Sequential Authentication. Authentication Order sets the preferred order for which the defined authentication methods are applied when a remote user logs on using the secondary logon page into the Portal.

To configure Authentication Order, perform the following:

1. **Log on to the BBI as administrator.**
2. **Select Config.**
3. **From the System tree view, select VPN Gateways.**

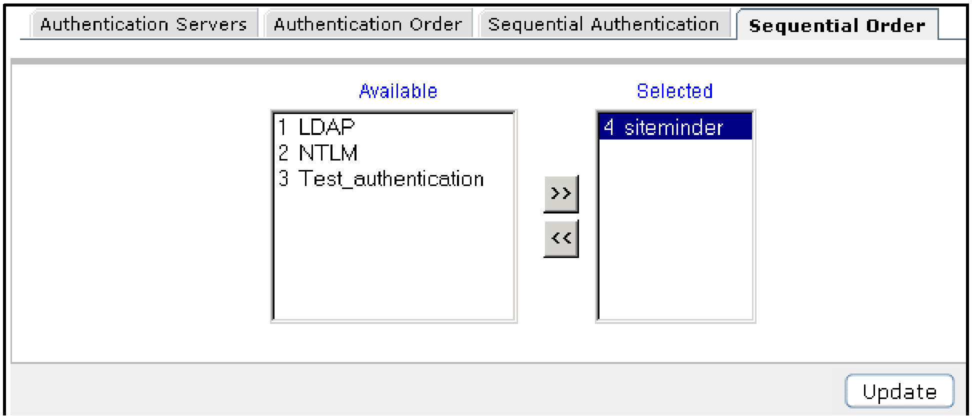
   The VPN Gateways form appears.

4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**
6. **Select Sequential Order.**

   The Sequential Order form appears.



7. **From the Available list, select `4 SiteMinder`.**
8. **Click >> to move the item to the Selected list.**
9. **Click Update.**
10. **Apply changes.**

RSA ClearTrust Authentication

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

The Avaya 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 Avaya VPN Gateway.

Configure Basic Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

   Authentication Server screen is displayed.

6. **Click Add.**

   Add New Authentication server is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

9. **Enter the Display name for the server.**

   This is an optional field.

10. **Select cleartrust in Mechanism drop-down list.**
11. **Click Update.**

    A new authentication ID is created.

Configure ClearTrust Settings

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

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

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

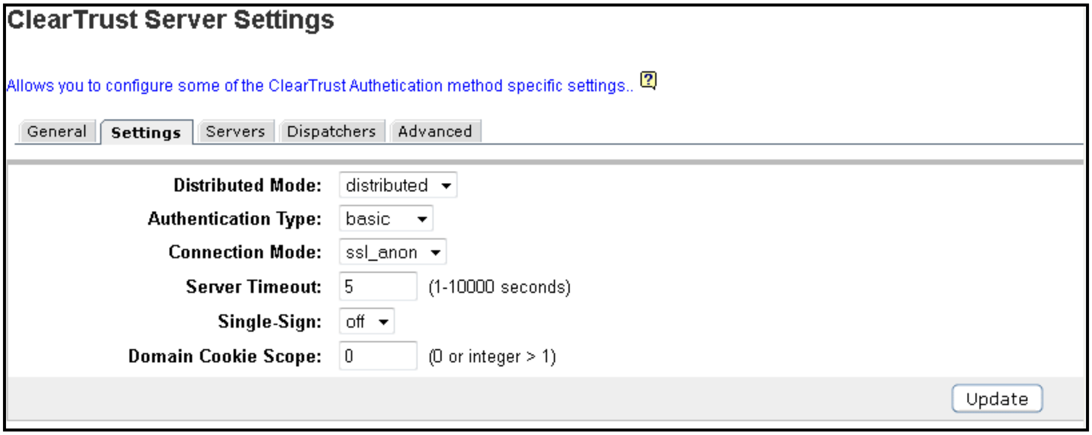
   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

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

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

14. Click the Settings tab.

The ClearTrust Server Settings form appears.



ClearTrust Server Settings

Allows you to configure some of the ClearTrust Authetication method specific settings..

Distributed Mode:	distributed
Authentication Type:	basic
Connection Mode:	ssl_anon
Server Timeout:	5 (1-10000 seconds)
Single-Sign:	off
Domain Cookie Scope:	0 (0 or integer > 1)

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 Avaya VPN Gateway.

- `standard`: The Avaya VPN Gateway sends requests to the first available ClearTrust authorization server.
- `distributed`: The Avaya VPN Gateway 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 Avaya 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 Avaya 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 Avaya 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 (e.g. `vpn.example.com`) and the other ClearTrust-enabled site (e.g. `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 Avaya 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 Avaya 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 (see above) 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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

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

A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

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

12. **Click Update.**

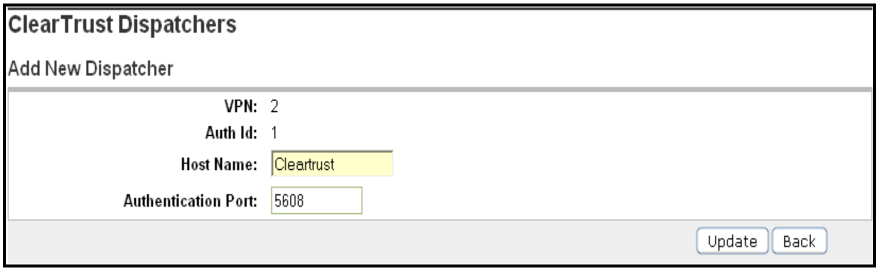
    A new authentication ID is created.

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

14. **Click the Dispatchers tab.**

15. **Click Add.**

    The Add New Dispatcher form is displayed.



ClearTrust Dispatchers

Add New Dispatcher

VPN:	2
Auth Id:	1
Host Name:	Cleartrust
Authentication Port:	5608

16. **In the Host Name field, enter the host name of a ClearTrust dispatcher.**

    This step lets you point out one or several *Dispatcher*s 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 Avaya VPN Gateway) communicate directly with the authorization server(s). Note that if a dispatcher is configured on the Avaya VPN Gateway, any authorization servers configured on the Avaya VPN Gateway will be ignored.

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

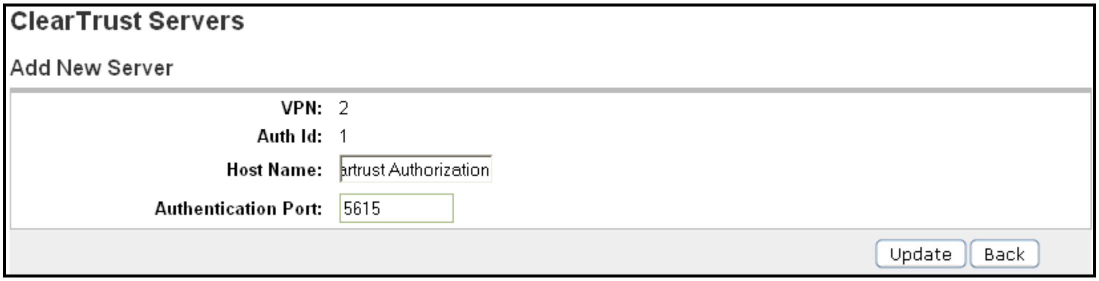
   Add New Authentication server form is displayed.
8. **Select the Auth ID.**
9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

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

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

14. **Click on Authorization tab.**



ClearTrust Servers

Add New Server

VPN:	2
Auth Id:	1
Host Name:	artrust Authorization
Authentication Port:	5615

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 the section “RSA ClearTrust Authentication” on page 301.

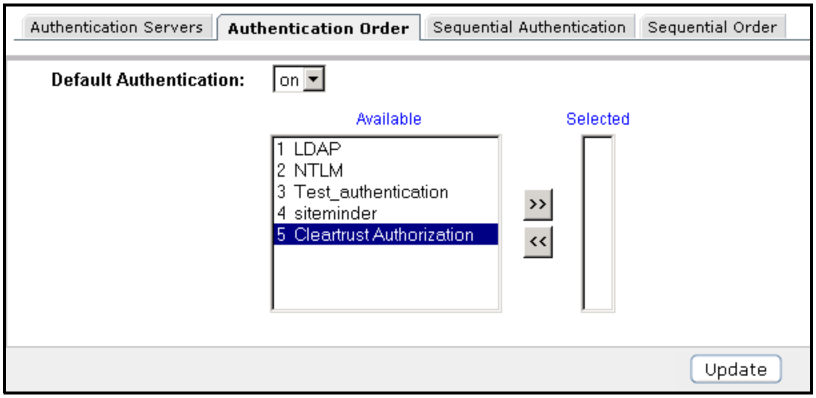
Specify the Authentication Fallback Order

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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
6. **Click the Authentication Order tab.**

   The Authentication Order form appears.



Default Authentication: on

Available

1 LDAP
2 NTLM
3 Test_authentication
4 siteminder
5 Cleartrust Authorization

Selected

7. **From the Default Authentication list, select on to enable the default logon.**
The Login Service list appears in the Portal logon page.

Or

Select off to disable the default logon.
The configured authentication methods in the authentication order appears in the logon page. The authentication methods must contain a display name when the Default Authentication is off.

8. **Under Fallback Order, in the Available list, select `5 Cleartrust Authorization`.**

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 Avaya VPN Gateway ignores the other specified authentication methods (if any) in the Authentication Order list.

Configure Sequential Authentication

Sequential Authentication provides enhanced security by prompting dual authentication credentials to gain access to the portal. The portal presents two distinct logon pages for authenticating two authentication servers sequentially. After successful authentication of the primary authentication server, the second logon screen appears for Secondary Authentication. If the Secondary Authentication fails, retries are allowed before switching back to the primary logon screen. Secondary Authentication is for each VPN setting. The Secondary Authentication is limited to portal users, and is not supported for IPSec and Net Direct installed client users.

IPSec Two Factor authentication method provides support for IPSec and Net Direct 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. With this option you can enable both SSL Secondary Authentication and IPsec Two Factor authentication.

When configuring certificate authentication, IPsec Two Factor Authentication adds more security than SSL Secondary Authentication by requiring that the client provide 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.

To configure Sequential Authentication, perform the following:

1. **Log on to the BBI as administrator.**
2. **Select Config.**
3. **From the System tree view, select VPN Gateways.**

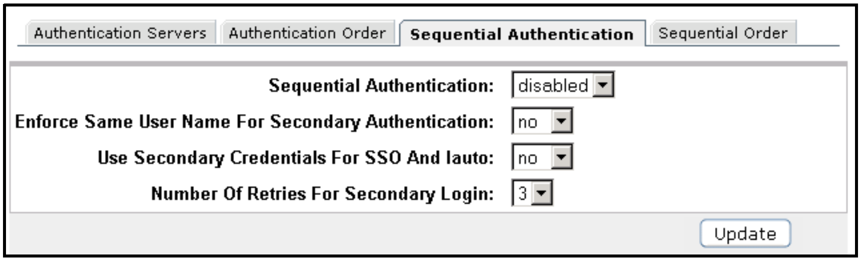
   The VPN Gateways form appears.

4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**
6. **Select Sequential Authentication.**

   The Sequential Authentication Order form appears.



Sequential Authentication: disabled

Enforce Same User Name For Secondary Authentication: no

Use Secondary Credentials For SSO And Iauto: no

Number Of Retries For Secondary Login: 3

7. **From the Sequential Authentication list, select enabled.**
8. **From the Enforce Same User Name For Secondary Authentication list, select yes to automatically update the user name field in the secondary logon page with the primary authentication user name. You cannot change the user name field value.**

   Or

   Select no, to enter the user name field in the secondary logon page.

9. **From the Use Secondary Credentials For SSO And Iauto list, select yes.**
10. **From the Number Of Retries For Secondary Login list, select the number of retries.**
11. **Click Update.**
12. **Click Apply.**

Specify Authentication Order

Sequential Authentication Order is applicable when you enable Sequential Authentication. Authentication Order sets the preferred order for which the defined authentication methods are applied when a remote user logs on using the secondary logon page into the Portal.

To configure Authentication Order, perform the following:

1. **Log on to the BBI as administrator.**
2. **Select Config.**
3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

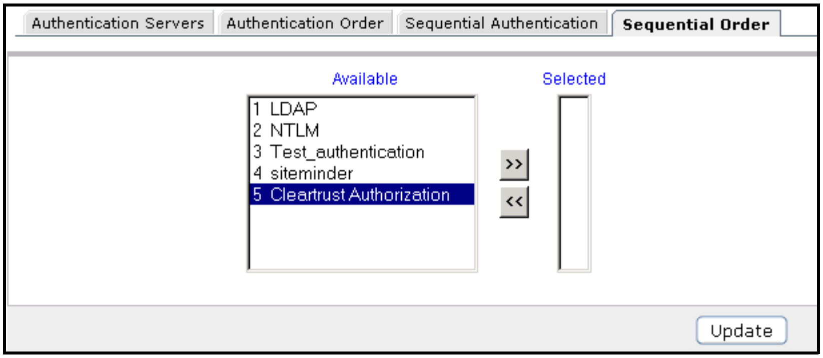
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**

6. **Select Sequential Order.**

   The Sequential Order form appears.



1 LDAP
2 NTLM
3 Test_authentication
4 siteminder
5 Cleartrust Authorization

7. **From the Available list, select `5 ClearTrust Authorization`.**

8. **Click >> to move the item to the Selected list.**

9. **Click Update.**

10. **Apply changes.**

RSA SecurID Authentication

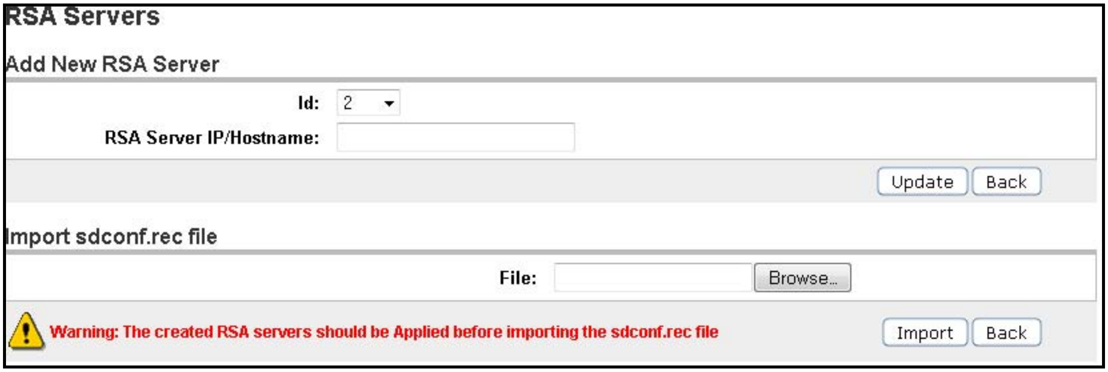
The RSA SecurID authentication method lets you configure user authentication through an existing RSA SecurID server.

Add RSA Server(s)

This description explains how to configure an RSA server under the system's global settings. If a Secure Service Partitioning license is loaded, it is also possible to configure the RSA server for a specific VPN, under VPN Gateways>VPN #>RSA Servers.

1. **In the System tree view, expand Administration.**
2. **Select RSA Servers and click Add.**

   The Add New RSA Server form is displayed.



RSA Servers

Add New RSA Server

Id: 2

RSA Server IP/Hostname:

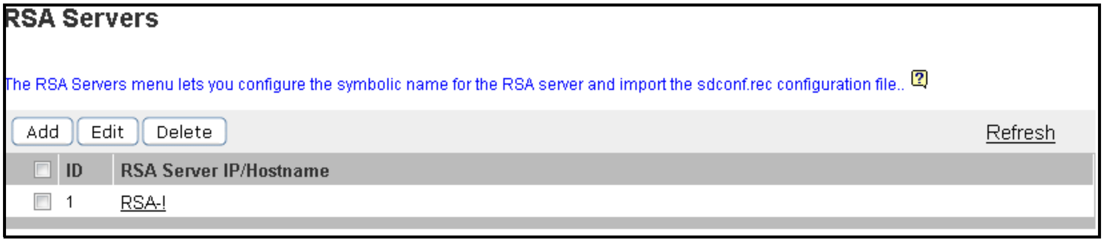
Import sdconf.rec file

File:

Warning: The created RSA servers should be Applied before importing the sdconf.rec file

3. **In the RSA Server IP/Hostname field, enter a symbolic name for the new RSA server.**
4. **Click Update.**

The RSA Servers form reappears.



RSA Servers

The RSA Servers menu lets you configure the symbolic name for the RSA server and import the sdconf.rec configuration file..

□	ID	RSA Server IP/Hostname
□	1	RSA-I

Configure Basic Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

   Authentication Server screen is displayed.

6. **Click Add.**

   Add New Authentication server is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter a name for the authentication method, for example `rsa`.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter. For more information about client filters, see Chapter 8, “Groups, Access Rules and Profiles”.

9. **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, in the Avaya VPN Client 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.

   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.

10. **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 Chapter 11, "Group Links".

11. **Select rsa from the Mechanism list.**

12. **Click Update.**

    A new authentication ID is created.

Configure RSA Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server form is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

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

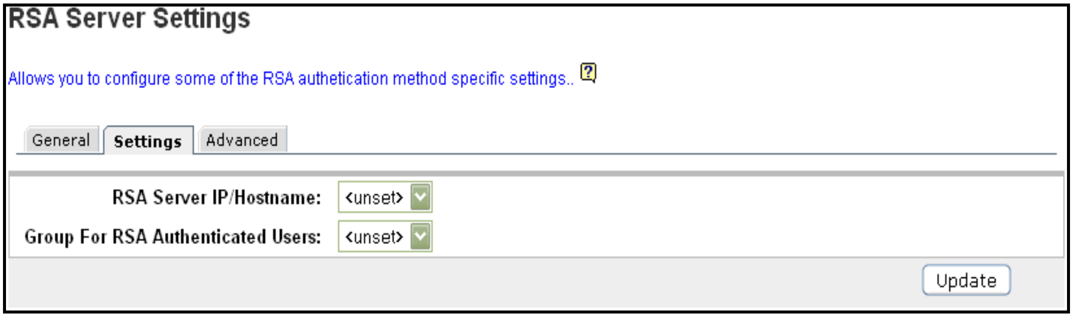
12. **Click Update.**

A new authentication ID is created.

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

14. **Click the Settings tab.**

    The RSA Server Settings form is displayed.



RSA Server Settings

Allows you to configure some of the RSA authetication method specific settings..

RSA Server IP/Hostname: <unset>

Group For RSA Authenticated Users: <unset>

15. **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 in the section “Configure Basic Settings” on page 315.

16. **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 Avaya VPN Gateway) to which authenticated users will be assigned. The access rules pertaining to this group will determine the user’s access rights.

17. **Click Update.**

18. **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 system administrator.**

2. **Click on Config tab.**

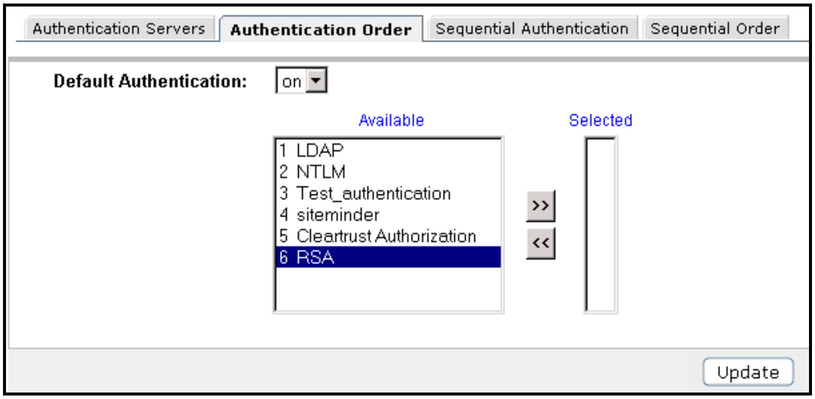
3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

6. **Click the Authentication Order tab.**

   The AuthOrder form is displayed.



Default Authentication: on

1 LDAP
2 NTLM
3 Test_authentication
4 siteminder
5 Cleartrust Authorization
6 RSA

7. **From the Default Authentication list, select on to enable the default logon.**
   The Login Service list appears in the Portal logon page.

   Or

   Select off to disable the default logon.
   The configured authentication methods in the authentication order appears in the logon page. The authentication methods must contain a display name when the Default Authentication is off.

8. **Under Fallback Order, in the Available list, select 6 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 Avaya VPN Gateway ignores the other specified authentication methods (if any) in the Authentication Order list.

Configure Sequential Authentication

Sequential Authentication provides enhanced security by prompting dual authentication credentials to gain access to the portal. The portal presents two distinct logon pages for authenticating two authentication servers sequentially. After successful authentication of the primary authentication server, the second logon screen appears for Secondary Authentication. If the Secondary Authentication fails, retries are allowed before switching back to the primary login screen. Secondary Authentication is for each VPN setting. The Secondary Authentication is limited to portal users, and is not supported for IPSec and Net Direct installed client users.

IPSec Two Factor authentication method provides support for IPSec and Net Direct 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. With this option you can enable both SSL Secondary Authentication and IPsec Two Factor authentication.

When configuring certificate authentication, IPsec Two Factor Authentication adds more security than SSL Secondary Authentication by requiring that the client provide 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 – The RSA SecurID New Pin mode is not supported when using Secondary Authentication service.

To configure Sequential Authentication, perform the following:

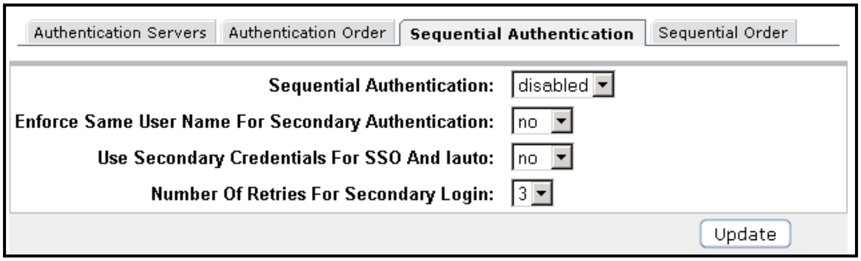
1. **Log on to the BBI as administrator.**
2. **Select Config.**
3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.
5. **Select Authentication.**

6. **Select Sequential Authentication.**

   The Sequential Authentication Order form appears.



Sequential Authentication: disabled

Enforce Same User Name For Secondary Authentication: no

Use Secondary Credentials For SSO And Iauto: no

Number Of Retries For Secondary Login: 3

7. **From the Sequential Authentication list, select enabled.**

8. **From the Enforce Same User Name For Secondary Authentication list, select yes to automatically update the user name field in the secondary logon page with the primary authentication user name.**
   You cannot change the user name field value.

   Or

   Select no, to enter the user name field in the secondary logon page.

9. **From the Use Secondary Credentials For SSO And Iauto list, select yes.**

10. **From the Number Of Retries For Secondary Login list, select the number of retries.**

11. **Click Update.**

12. **Click Apply.**

Specify Authentication Order

Sequential Authentication Order is applicable when you enable Sequential Authentication. Authentication Order sets the preferred order for which the defined authentication methods are applied when a remote user logs on using the secondary logon page into the Portal.

To configure Authentication Order, perform the following:

1. **Log on to the BBI as administrator.**

2. **Select Config.**

3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

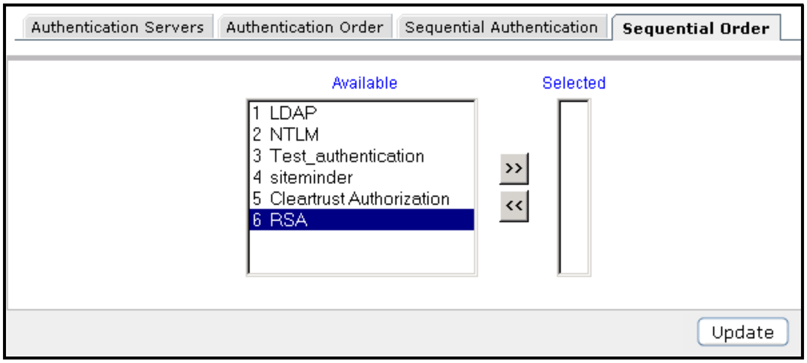
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**

6. **Select Sequential Order.**

   The Sequential Order form appears.



1 LDAP
2 NTLM
3 Test_authentication
4 siteminder
5 Cleartrust Authorization
6 RSA

7. **From the Available list, select `6 RSA`.**

8. **Click >> to move the item to the Selected list.**

9. **Click Update.**

10. **Apply changes.**

Local Database Authentication

The Avaya VPN Gateway 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 run 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. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

   Authentication Server screen is displayed.

6. **Click Add.**

   Add New Authentication server is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter a name for the authentication method, for example `local`.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter. For more information about client filters, see Chapter 8, "Groups, Access Rules and Profiles".

9. **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, in the Avaya VPN Client 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.

   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.

10. **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 Chapter 11, "Group Links".

11. **Select local from Mechanism drop-down list.**

12. **Click Update.**

    Before you start adding users to the local database, you must configure the authentication order. For more information about the configuration, see "Specify the Authentication Fallback Order" on page 323.

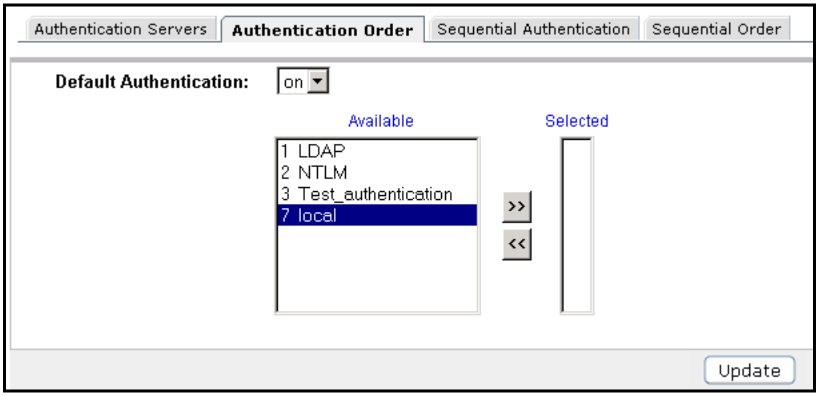
Specify the Authentication Fallback Order

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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
6. **Click the Authentication Order tab.**

   The AuthOrder form is displayed.



Default Authentication: on

Available

1 LDAP
2 NTLM
3 Test_authentication
7 local

Selected

7. **From the Default Authentication list, select on to enable the default logon.**
   The Login Service list appears in the Portal logon page.

   Or

   Select off to disable the default logon.
   The configured authentication methods in the authentication order appears in the logon page. The authentication methods must contain a display name when the Default Authentication is off.

8. **Under Fallback Order, in the Available list, select `7 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 Avaya VPN Gateway ignores the other specified authentication methods (if any) in the Authentication Order list.

Configure Sequential Authentication

Sequential Authentication provides enhanced security by prompting dual authentication credentials to gain access to the portal. The portal presents two distinct logon pages for authenticating two authentication servers sequentially. After successful authentication of the primary authentication server, the second logon screen appears for Secondary Authentication. If the-Secondary Authentication fails, retries are allowed before switching back to the primary logon screen. Secondary Authentication is for each VPN setting. The Secondary Authentication is limited to portal users, and is not supported for IPSec and Net Direct installed client users.

IPSec Two Factor authentication method provides support for IPSec and Net Direct 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. With this option you can enable both SSL Secondary Authentication and IPsec Two Factor authentication.

When configuring certificate authentication, IPsec Two Factor Authentication adds more security than SSL Secondary Authentication by requiring that the client provide 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.

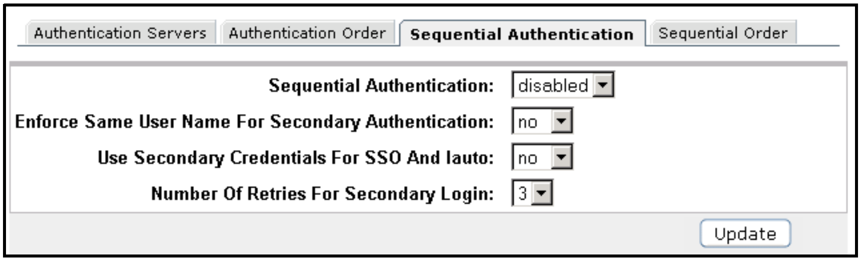
To configure Sequential Authentication, perform the following:

1. **Log on to the BBI as administrator.**
2. **Select Config.**
3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.
5. **Select Authentication.**
6. **Select Sequential Authentication.**

   The Sequential Authentication Order form appears.



Sequential Authentication: disabled
Enforce Same User Name For Secondary Authentication: no
Use Secondary Credentials For SSO And Iauto: no
Number Of Retries For Secondary Login: 3

7. **From the Sequential Authentication list, select enabled.**
8. **From the Enforce Same User Name For Secondary Authentication list, select yes to automatically update the user name field in the secondary logon page with the primary authentication user name.**
   You cannot change the user name field value.

   Or

   Select no, to enter the user name field in the secondary logon page.
9. **From the Use Secondary Credentials For SSO And Iauto list, select yes.**
10. **From the Number Of Retries For Secondary Login list, select the number of retries.**
11. **Click Update.**

12. **Click Apply.**

Specify Authentication Order

Sequential Authentication Order is applicable when you enable Sequential Authentication. Authentication Order sets the preferred order for which the defined authentication methods are applied when a remote user logs on using the secondary logon page into the Portal.

To configure Authentication Order, perform the following:

1. **Log on to the BBI as administrator.**

2. **Select Config.**

3. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

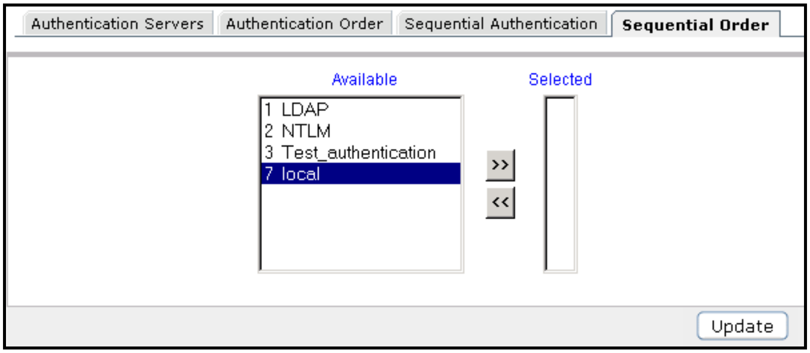
4. **Select the configured VPN for which you want to enable authentication.**

   The VPN Summary form appears.

5. **Select Authentication.**

6. **Select Sequential Order.**

   The Sequential Order form appears.



Available:
1 LDAP
2 NTLM
3 Test_authentication
7 local

7. **From the Available list, select `7 local`.**

8. **Click >> to move the item to the Selected list.**

9. **Click Update.**

10. **Apply changes.**

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 Avaya VPN Gateway. For instructions on group configuration, see Chapter 8, “Groups, Access Rules and Profiles”.

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

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

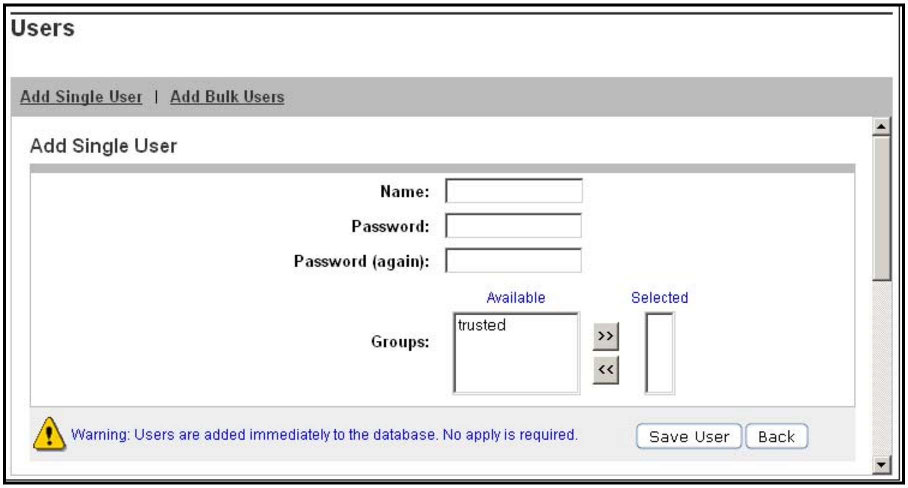
   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

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

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

    The Users form is displayed.

15. **Under Users, click Add.**



Users

Add Single User | Add Bulk Users

Add Single User

Name:

Password:

Password (again):

Groups: Available: trusted — Selected:

Warning: Users are added immediately to the database. No apply is required.

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 328.

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 may be to paste or enter a bulk of users (with passwords and groups) into the box displayed when clicking **Add Bulk Users**.

1. **Enter the users on separate rows according to the following format:**

    john:password:group1,group2
    lisa:password:group1,group2,group3

2. **Click Save Users.**

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 system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

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

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

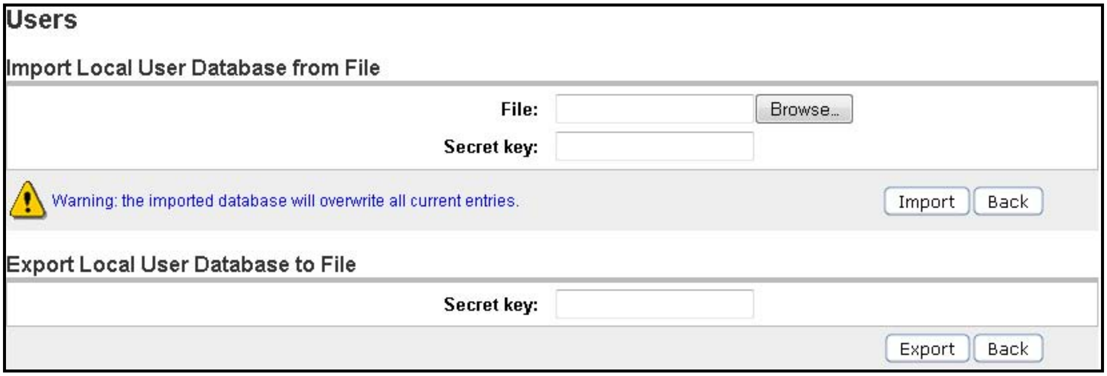
    This is an optional field.
11. **Select local in Mechanism drop-down list.**
12. **Click Update.**

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

The Users form is displayed.

15. **In the Users form, click the Import/Export button.**

    The Import/Export Local User Database from File form is displayed.



Users

Import Local User Database from File

File:

Secret key:

Warning: the imported database will overwrite all current entries.

Export Local User Database to File

Secret key:

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 system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server form is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

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

12. **Click Update.**

    A new authentication ID is created.

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

14. **Click the Users tab.**

    The Users form is displayed.

15. **In the Users form, click the Import/Export button.**

    The Import/Export Local User Database from File form is displayed.

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 Avaya 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. **In the System tree view, select VPN Gateways.**
2. **Select the VPN Gateway name for configuring the authentication.**
3. **Under settings, select Authentication.**
   Authentication Server screen is displayed.
4. **If the Authentication server is already present go to Step 11.**
5. **Click Add.**

   Add New Authentication server form is displayed.
6. **Select the Auth ID.**
7. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
8. **Enter the Display name for the server.**

   This is an optional field.
9. **Select local in Mechanism drop-down list.**
10. **Click Update.**

    A new authentication ID is created.
11. **Click the Authentication ID in the Authentication Server screen.**
12. **Click the Users tab.**
13. **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.
14. **In the Max list box, select the maximum number of users to display.**
15. **Click the List button.**

    Registered users are displayed.

Configure user password change settings

This section provides instructions to configure user password change settings.

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

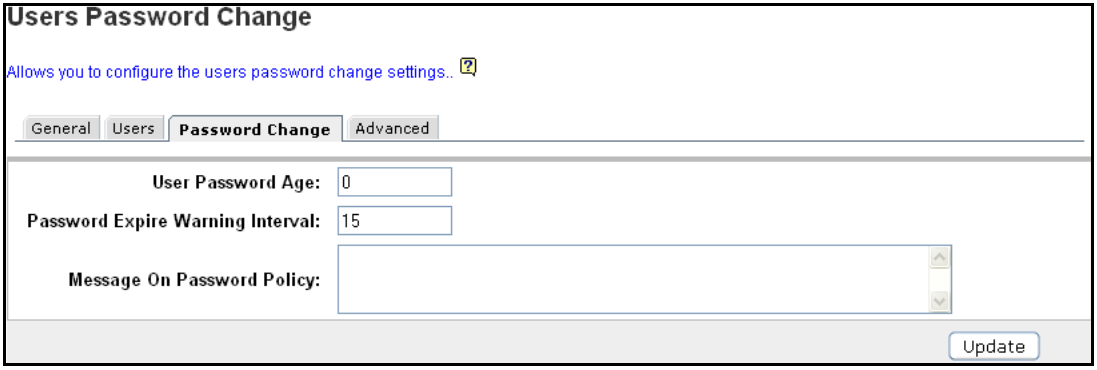
   Under settings, select Authentication.
   Authentication Server screen is displayed.
3. **If the Authentication server is already present go to Step 11.**
4. **Click Add.**

   Add New Authentication server form is displayed.
5. **Select the Auth ID.**
6. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.
7. **Enter the Display name for the server.**

   This is an optional field.
8. **Select local in Mechanism drop-down list.**
9. **Click Update.**

   A new authentication ID is created.
10. **Click the Authentication ID in the Authentication Server screen**
11. **Click the Password Change tab.**



Users Password Change

Allows you to configure the users password change settings..

User Password Age: 0

Password Expire Warning Interval: 15

Message On Password Policy:

12. **Specify the age for user password.**
    This age is used to calculate the password expire option. Default value will be 0, so that the password will never expire.

13. **Specify the password expiry notification warning interval.**
    If this is set to 0, no warning will be given. Otherwise, a warning message will be displayed on the portal when password expiry time is within the interval specified here. Default value is 15.

14. **Specify the password text to be displayed to the user in the change password page.**

15. **Click Update to submit the specified settings to the pending configuration.**

Client Certificate Authentication

With client certificate authentication enabled on the Avaya VPN Gateway, login to the VPN is not required for remote users with a valid client certificate installed on their computers. Once the Avaya VPN Gateway has accepted the certificate, the user is granted access to the VPN. Client certificate authentication is also considered more secure.

To enable client certificate authentication, the following steps need to be completed:

- Generate unique client certificates
- Configure client certificate authentication
- Configure the VPN to ask for client certificates

Generate Unique Client Certificates

Each user should be provided with a unique client certificate, generated from a CA certificate. The certificates can be generated by an external certificate management tool or by using the commands available on the Avaya VPN Gateway. The CA certificate must however be installed on the Avaya VPN Gateway.

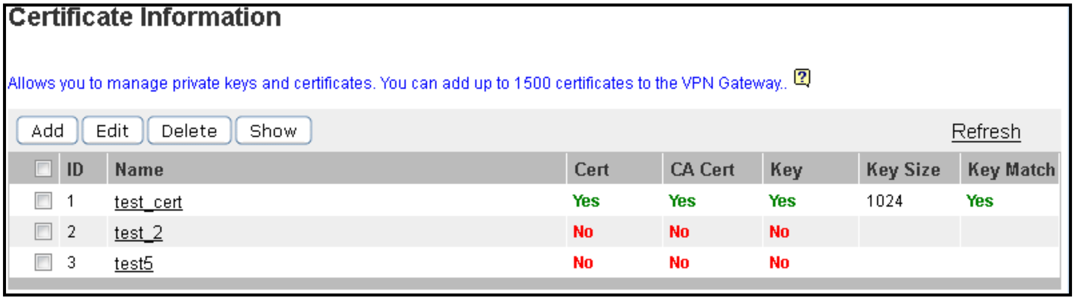
For general instructions on Avaya VPN Gateway certificate management (for example how to add certificates to the Avaya VPN Gateway and how to use the Avaya VPN Gateway to generate client certificates), see the "Certificates and Client Authentication" chapter in the *User's Guide*.

To authenticate a user with a client certificate, the Avaya VPN Gateway extracts user name and group membership information from the client certificate's subject part. No password information is required. Before you generate the client certificate, you should determine which entries in the subject part that should be used for extracting this information.

The Avaya VPN Gateway provides the way to print a certificate's subject entries:

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the system tree view, select Certificates**

Certificates added to the Avaya VPN Gateway are displayed.



Certificate Information

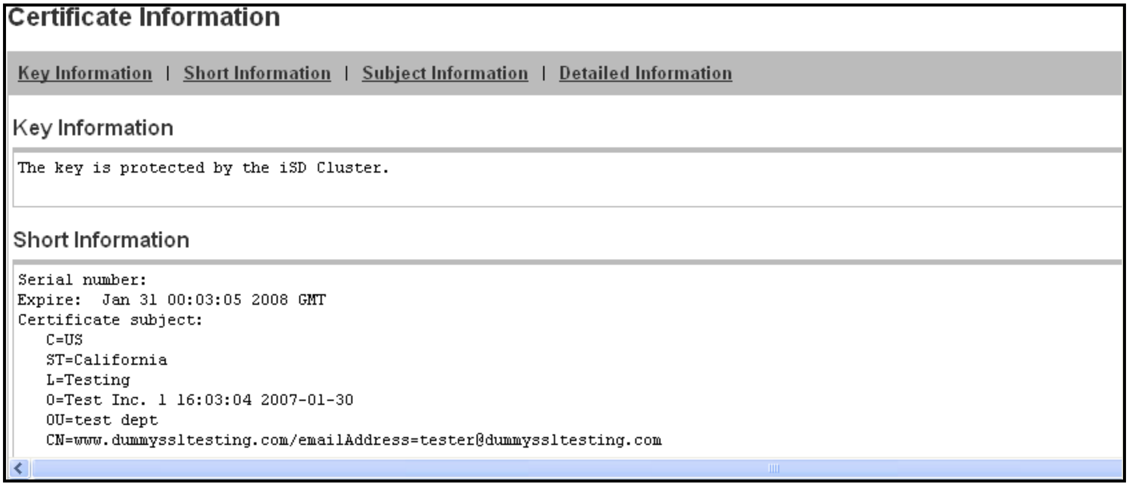
Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		

4. **Select the check box next to the certificate Name.**

5. **Click Show.**

   The certificate is shown. The subject part of the certificate is displayed at the top.



Certificate Information

Key Information | Short Information | Subject Information | Detailed Information

Key Information

```
The key is protected by the iSD Cluster.
```

Short Information

```
Serial number:
Expire:  Jan 31 00:03:05 2008 GMT
Certificate subject:
   C=US
   ST=California
   L=Testing
   O=Test Inc. 1 16:03:04 2007-01-30
   OU=test dept
   CN=www.dummyssltesting.com/emailAddress=tester@dummyssltesting.com
```

The left column shows available entries. The right column shows the values specified for the CA certificate. When generating the client certificate you will be prompted for new values for the same entries.

- ***User name***. You can for example use the `CN/commonName` entry to extract user name. Then, as you generate a client certificate for a specific user, enter the user name of that user when prompted for Common Name. Make a note of the OID (object identifier), in this case 2.5.4.3. The OID should later be configured in the BBI (see page 343).

- ***Group name***. To map the user to access groups (as defined on the Avaya VPN Gateway), choose one or several entries to use for extraction of group names. Then, as you generate a client certificate for the user, enter the group name when prompted for the entry you have decided to use for group name. Make a note of the OID(s). They should later be configured in the BBI (see page 342).

NOTE – The iauto link (described in Chapter 11, "Example 5a: Automatic Login Link Secured by the Avaya VPN Gateway (Iauto)") can be used together with client certificate authentication, but only if the backend server does not require a password. Only the user and domain credentials will be passed to the backend server when client certificate authentication is used.

Mapping Group Names to CA Certificate

Instead of extracting group names from the user's client certificate, they can be retrieved from the CA certificates that were used to generate the client certificates. The trick is to use several different CA certificates, where each CA certificate represents a user access group. One CA certificate could for example represent the engineering group and another the accounting group.

To generate client certificates for a specific group, simply use the CA certificate you have in mind for this group. No modifications need to be made to the CA certificates. Then map the CA certificate to the group, using the `cacerts` command (see page 341).

NOTE – The CA certificate that was used to generate the client certificates must be installed on the Avaya VPN Gateway. For instructions on how to add certificates to the Avaya VPN Gateway, see the "Certificates and Client Authentication" chapter in the *User's Guide*.

This method can be combined with the method described in the previous section. The group names retrieved from the CA certificate will be appended to those extracted from the client certificate. Note that all group names have to be defined on the Avaya VPN Gateway with access rules. See Chapter 8, "Groups, Access Rules and Profiles".

If a default group is specified, this group name will be assigned to the user if no other group has been configured. To specify a default group, start by configuring a group with the desired access rules (for instructions on group configuration, see Chapter 8, "Groups, Access Rules and Profiles"). Then select this group the default group in the **Default Group** list box (**VPN Gateways>VPN #>Group Settings>Groups**).

Configure Client Certificate Authentication

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**

   Authentication Server screen is displayed.

6. **Click Add.**

   Add New Authentication server is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter a name for the authentication method, for example `cert`.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter. For more information about client filters, see Chapter 8, “Groups, Access Rules and Profiles”.

9. **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 Chapter 11, “Group Links”.

10. **Select cert in Mechanism drop-down list.**

11. **Click Update.**

Configure Certificate Settings

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   Authentication Server screen is displayed.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   Add New Authentication server form is displayed.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

   A name is mandatory. To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

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

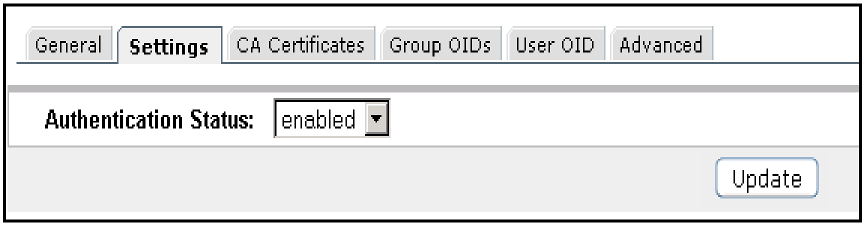
12. **Click Update.**

    A new authentication ID is created.

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

14. **Click the Settings tab.**

    The Cert Server Settings form is displayed.



Authentication Status: enabled

15. **In the Authentication Status list box, verify that `enabled` is selected.**

    Using this setting, you can you temporarily disable client certificate authentication if necessary. Once you reenable the client certificate authentication, you do not have to configure all the settings for the current authentication ID once again.

16. **Click Update.**

Configure CA Certificates

Read this section if you want to map user groups to the CA certificates that were used to generate the client certificates (see the notes on page 337).

Example: If you have chosen to generate client certificates for the `engineering` group from CA certificate 1, map the `engineering` group to this certificate.

If you want to extract the group name from the client certificate, read the next section.

1. **Log on as system administrator.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   Authentication Server screen is displayed**.**
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

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

   A name is mandatory.To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

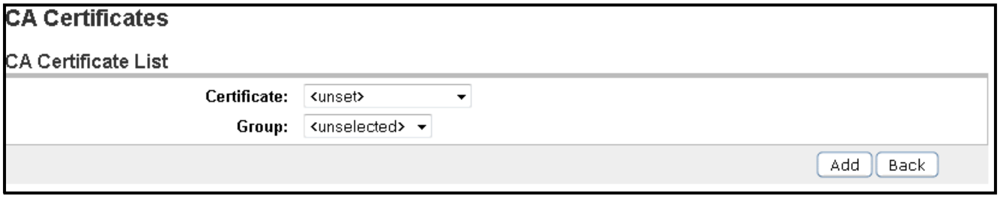
    This is an optional field.
11. **Select cert in Mechanism drop-down list.**
12. **Click Update.**

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

    The CA Certificates form is displayed.

15. **Click Add.**

    The CA Certificate List form is displayed.



CA Certificates

CA Certificate List

Certificate: <unset>

Group: <unselected>

16. **In the Certificate Number list box, select the desired CA certificate.**

    The CA certificates that were used to generate the client certificates must be imported to the Avaya VPN Gateway, otherwise they will not be displayed in the list box.

17. **In the Group list box, select the group to which the CA certificate should be mapped.**

18. **Click Add.**

19. **Apply the changes.**

Configure Group OIDs

Read this section if you are extracting group names from entries in the client certificates.

1. **Log on as system administrator.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

    Under settings, select Authentication.
    Authentication Server screen is displayed.

5. **If the Authentication server is already present go to Step 12.**

6. **Click Add.**

    Add New Authentication server form is displayed.

7. **Select the Auth ID.**

8. **In the Name field, enter the Authentication server name.**

    A name is mandatory. To refer the current authentication method, use this server name in the client filter.

9. **Enter the Display name for the server.**

   This is an optional field.

10. **Select cert in Mechanism drop-down list.**

11. **Click Update.**

    A new authentication ID is created.

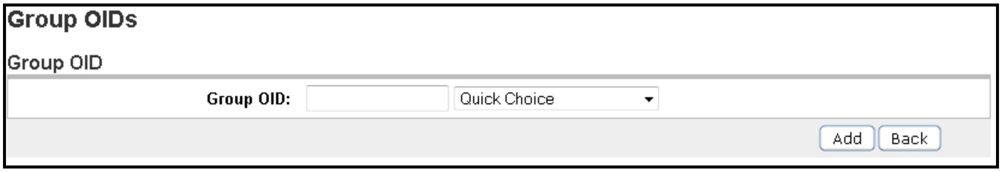
12. **Click the Authentication ID in the Authentication Server screen.**

13. **Click the Group OIDs Certificate tab.**

    The Group OIDs form is displayed.

14. **Click Add.**

    The Group OID form is displayed.



Group OIDs

Group OID

Group OID: Quick Choice

15. **In the Group OID field, specify the desired groupOID.**

    The value corresponding to this OID will be extracted from the client certificate as group name. The Quick Choice list box lets you select items from a list of possible OIDs.

    OIDs can be specified either as the symbolic name (for example localityName) or as the OID (for example 2.5.4.7).

16. **Click Add.**

17. **Apply the changes.**

Configure User OID

The U.S. Department of Defense Common Access Card (CAC) contains the client certificate which requires special manipulation to use Microsoft user principal name (UPN). Whereas, other users (non CAC users) can use the UPN through support for SubjectAltName which was added in this release.

For more information about the configuration, see the following:

- "Configuring the subject name" on page 343
- "Appending string value to subject name" on page 344
- "Configuring the subject alternative name" on page 346

Configuring the subject name

To extract the User OID based on subject name, perform the following procedure:

1. **Log on as a system administrator.**
2. **Click the Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   The Authentication Server screen appears.
6. **If the Authentication server is already present, go to Step 13.**
7. **Click Add.**

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

   To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

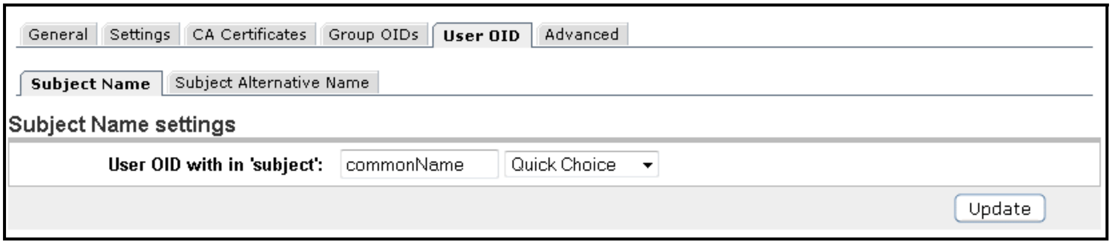
    This is an optional field.
11. **From the Mechanism list, select cert.**
12. **Click Update.**

    An authentication ID is created.

13. **Click the Authentication ID in the Authentication Server form.**

14. **Click the User OID tab.**

    The User OID form appears.



User OID with in 'subject': commonName

15. **Select the Subject Name tab.**

16. **In the User OID with in 'subject' field, enter the subject name or from the Quick Choice list, select the subject name.**

    Extracts the user from general names inside the subject name.

17. **Click Update.**

18. **Apply the changes.**

Appending string value to subject name

To append string value to subject name, perform the following procedure:

1. **Log on as a system administrator.**

2. **Click the Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN Gateway name for configuring the authentication.**

5. **Under settings, select Authentication.**
   The Authentication Server screen appears.

6. **If the Authentication server is already present go to Step 13.**

7. **Click Add.**

   The Add New Authentication server form appears.

8. **Select the Auth ID.**

9. **In the Name field, enter the Authentication server name.**

To refer the current authentication method, use this server name in the client filter.

10. **Enter the Display name for the server.**

    This is an optional field.

11. **From the Mechanism list, select cert.**

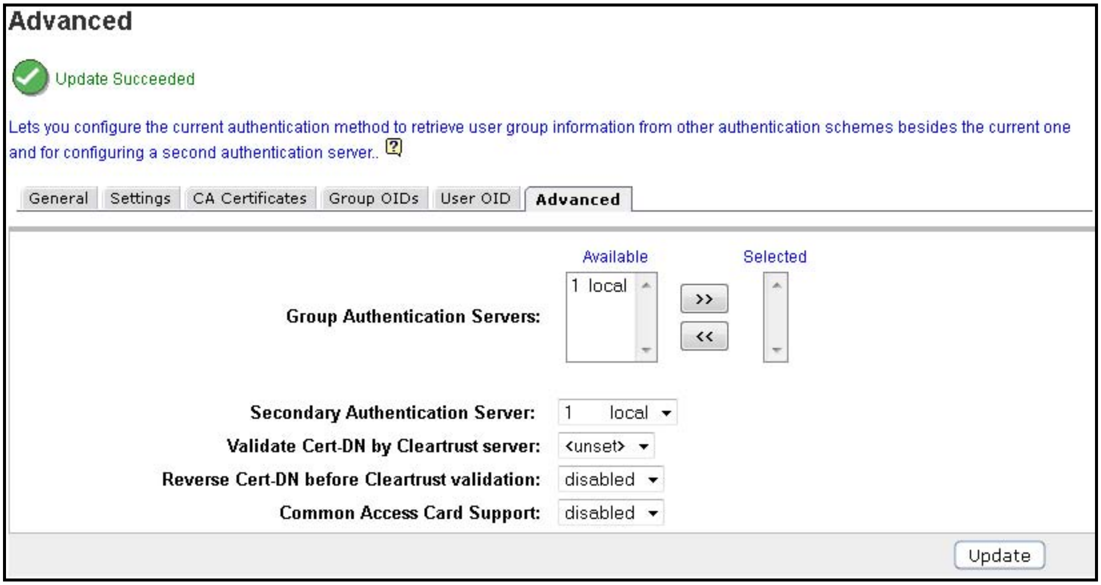
12. **Click Update.**

    An authentication ID is created.

13. **Click the Authentication ID in the Authentication Server form.**

14. **Click the Advanced tab.**

    The Advanced form appears.



Advanced

Update Succeeded

Lets you configure the current authentication method to retrieve user group information from other authentication schemes besides the current one and for configuring a second authentication server..

Group Authentication Servers: 1 local

Secondary Authentication Server: 1 local

Validate Cert-DN by Cleartrust server: <unset>

Reverse Cert-DN before Cleartrust validation: disabled

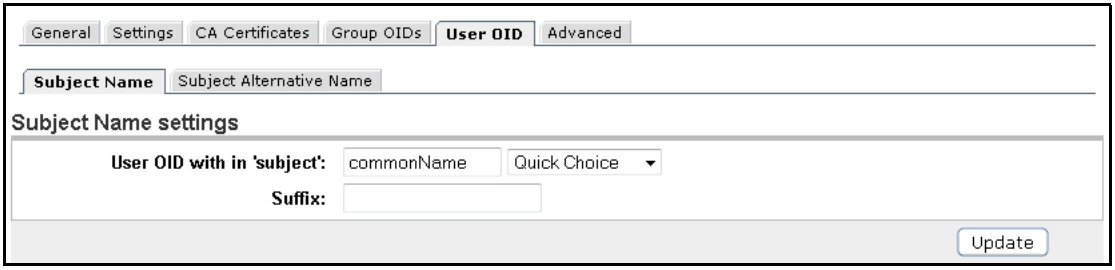
Common Access Card Support: disabled

15. **From the Command Access Card Support list, select enabled.**

16. **Click Update.**

17. **Click the User OID tab.**

The User OID form appears.



Subject Name settings

User OID with in 'subject': commonName

Suffix:

18. **In the Suffix field, enter string value to the subject name.**

    The suffix must be commonName type only. Valid string value is up to 255 characters.

19. **Click Update.**

Configuring the subject alternative name

To extract the User OID based on subject alternative name, perform the following procedure:

1. **Log on as a system administrator.**
2. **Click the Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   The Authentication Server screen appears.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

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

   To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

    This is an optional field.
11. **From the Mechanism list, select cert.**

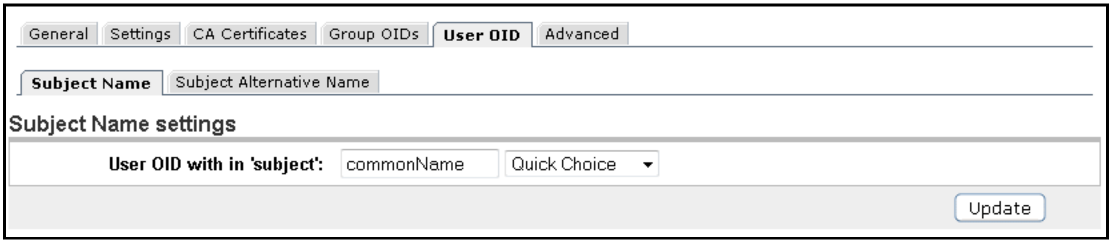
12. **Click Update.**

    An authentication ID is created.

13. **Click the Authentication ID in the Authentication Server form.**

14. **Click the User OID tab.**

    The User OID form appears.

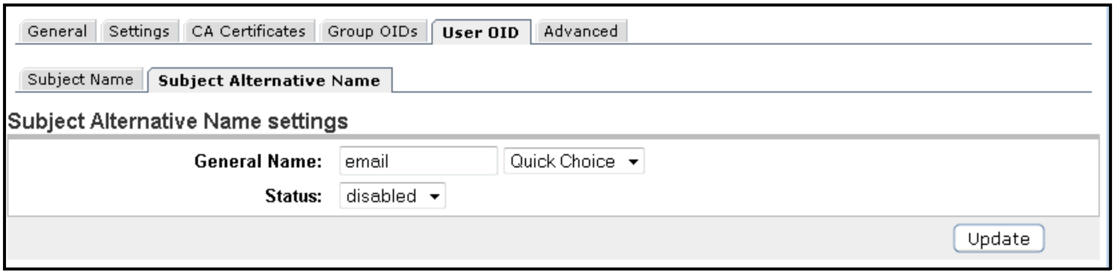


Subject Name settings

User OID with in 'subject': commonName

15. **Select the Subject Alternative Name tab.**

    The Subject Alternative Name settings form appears.



Subject Alternative Name settings

General Name: email

Status: disabled

16. **In the General Name field, enter the subject alternate name or from the Quick Choice list, select the subject alternate name.**

    The value corresponding to this subject alternate name is extracted from the client certificate as group name.

17. **From the Status list, select enabled.**

18. **Click Update.**

19. **Apply the changes.**

Configure Advanced settings

To configure advanced settings, perform the following procedure:

1. **Log on as a system administrator.**
2. **Click the Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN Gateway name for configuring the authentication.**
5. **Under settings, select Authentication.**
   The Authentication Server screen appears.
6. **If the Authentication server is already present go to Step 13.**
7. **Click Add.**

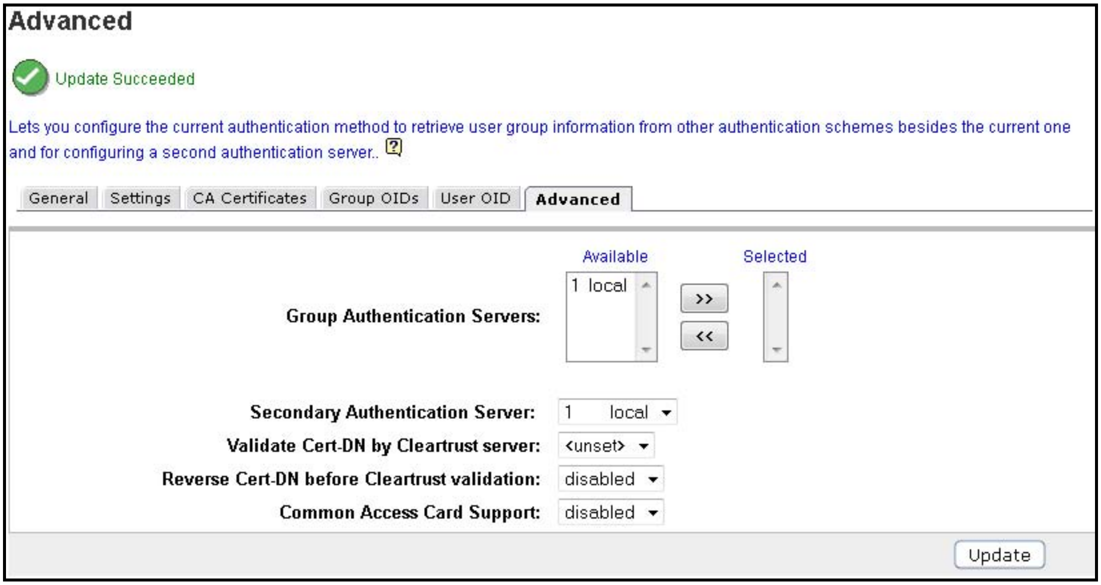
   The Add New Authentication server form appears.
8. **Select the Auth ID.**
9. **In the Name field, enter the Authentication server name.**

   To refer the current authentication method, use this server name in the client filter.
10. **Enter the Display name for the server.**

    This is an optional field.
11. **From the Mechanism list, select cert.**
12. **Click Update.**

    An authentication ID is created.
13. **Click the Authentication ID in the Authentication Server form.**
14. **Click the Advanced tab.**

The Advanced form appears.



Advanced

Update Succeeded

Lets you configure the current authentication method to retrieve user group information from other authentication schemes besides the current one and for configuring a second authentication server..

Group Authentication Servers: Available: 1 local

Secondary Authentication Server: 1 local

Validate Cert-DN by Cleartrust server: <unset>

Reverse Cert-DN before Cleartrust validation: disabled

Common Access Card Support: disabled

15. **From the Group Authentication Severs, select an available server from which to gather group ID information.**

16. **From the Secondary Authentication Servers, select a secondary authentication method.**

NOTE – IPsec Two Factor authentication supports only certificate authentication as primary and local, RADIUS or LDAP as secondary.

---

17. **From the Validate Cert-DN by Cleartrust server, select a Cleartrust authentication scheme.**

18. **From Reverse Cert-DN before Cleartrust validation, enable or disable Cleartrust reverse validation.**

19. **From the Command Access Card Support list, enable or disable the US Department of Defense Common Access Card support for certificate authentication.**

20. **Click Update.**

Configure the Portal Server

The portal server should have the relevant CA certificates installed and be configured to request client certificates.

1. **Install the CA certificate(s) used to generate the client certificates on the Avaya VPN Gateway.**

   If the CA certificate is not already installed on the Avaya VPN Gateway, it can be pasted or imported. Instructions in the "Adding Certificates to the Avaya VPN Gateway" section in the "Certificates and Client Authentication" chapter in the *User's Guide*.

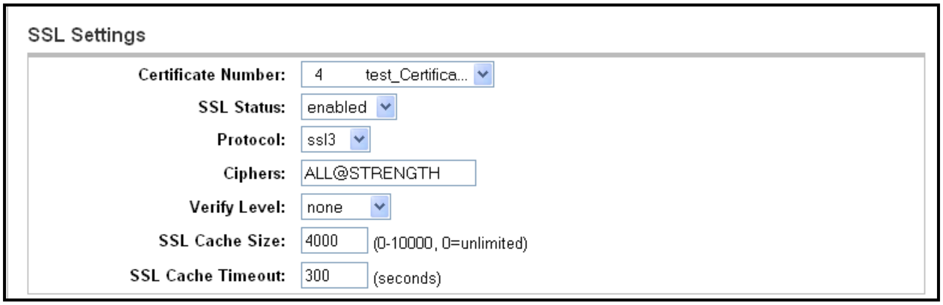
2. **In the System tree view, select VPN Gateways.**

3. **Select the VPN Gateway name.**

4. **Under Settings, select SSL.**

   The SSL form is displayed.

5. **Under General Settings, in the Verify Level list box, select `optional`.**

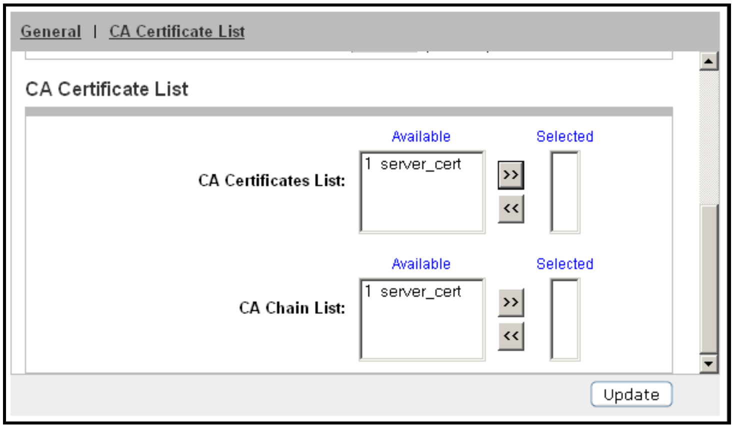


SSL Settings

Certificate Number:	4 test_Certifica...
SSL Status:	enabled
Protocol:	ssl3
Ciphers:	ALL@STRENGTH
Verify Level:	none
SSL Cache Size:	4000 (0-10000, 0=unlimited)
SSL Cache Timeout:	300 (seconds)

Optional means that the remote user will be prompted for a client certificate upon accessing the VPN. If the user does not have a client certificate or chooses not to use it for authentication, the Portal login page is displayed instead.

6. **Scroll down to the CA Certificate list (or click CA Certificate List on the gray area).**



CA Certificate List

CA Certificates List: Available: 1 server_cert; Selected:

CA Chain List: Available: 1 server_cert; Selected:

7. **In the CA Certificate list, move the desired CA certificate(s) to the Selected list.**

   This should be the CA certificate(s) used to generate the client certificates.

8. **Click Update.**

9. **Apply the changes.**

   If no other authentication method besides client certificate authentication is configured, your configuration will be more secure. Even though the Portal login page is displayed if a user cancels client certificate authentication, it is not possible to log in. This means that it is not possible to be logged in to the VPN without a client certificate.

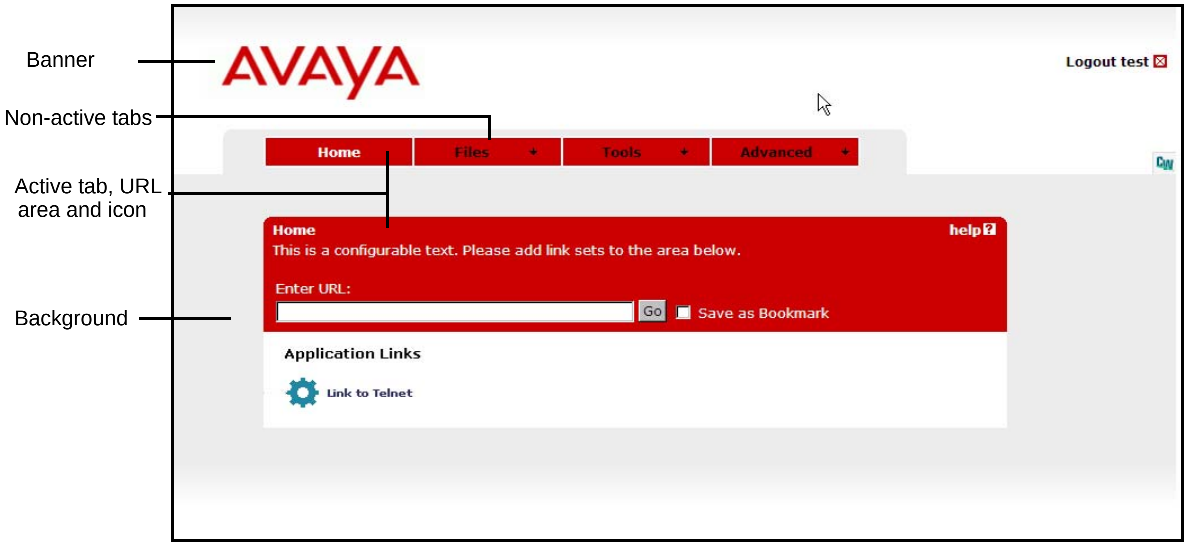
CHAPTER 10

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.



This is a configurable text. Please add link sets to the area below.

Enter URL:

Figure 10-1 Default Appearance

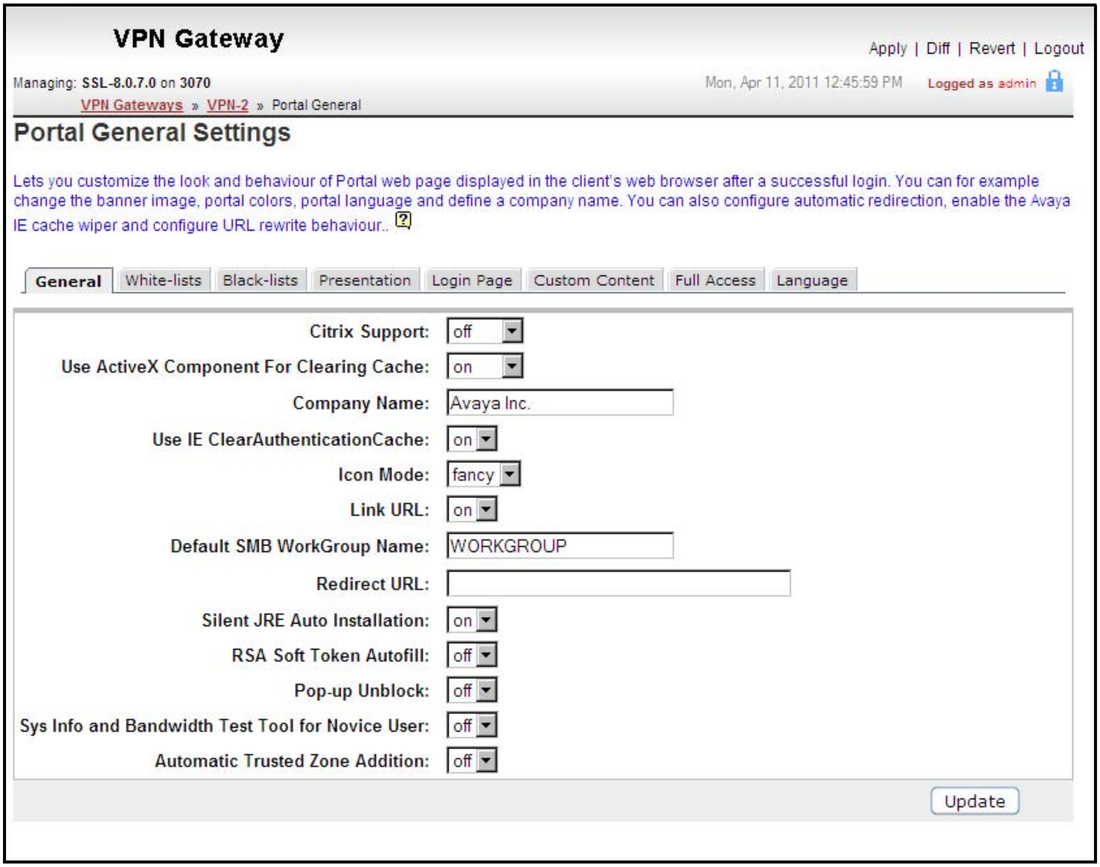
General Settings

The General Settings form lets you change a number of settings for the Portal.

1. **Log on to the BBI as administrator user.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN name from the Name list.**

   The VPN Summary screen is displayed.
5. **Under settings, select the Portal.**

   The Portal General Settings screen is displayed.



Managing: SSL-8.0.7.0 on 3070

Mon, Apr 11, 2011 12:45:59 PM

VPN Gateways » VPN-2 » Portal General

Portal General Settings

Lets you customize the look and behaviour of Portal web page displayed in the client's web browser after a successful login. You can for example change the banner image, portal colors, portal language and define a company name. You can also configure automatic redirection, enable the Avaya IE cache wiper and configure URL rewrite behaviour.. ?

Citrix Support:	off
Use ActiveX Component For Clearing Cache:	on
Company Name:	Avaya Inc.
Use IE ClearAuthenticationCache:	on
Icon Mode:	fancy
Link URL:	on
Default SMB WorkGroup Name:	WORKGROUP
Redirect URL:	
Silent JRE Auto Installation:	on
RSA Soft Token Autofill:	off
Pop-up Unblock:	off
Sys Info and Bandwidth Test Tool for Novice User:	off
Automatic Trusted Zone Addition:	off

6. **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 #>Group Settings>Groups>General** 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 Avaya VPN Gateway from starting the Java applet that supports this feature.

   Note: When `citrix` is set to `on` (on VPN level or group level), the Avaya VPN Gateway supports rewrite of ICA files only. Other methods are possible but may require configuration changes on the Citrix Metaframe server side.

7. **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 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 will be removed from the 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 #>Group Settings>Group>General** to enable or disable the 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#> SSL>HTTP>General**). The cache will however not be cleared.

8. **In the Company Name field, enter the desired company name.**

   This name will replace the default “Avaya Inc.” company name shown as a “tool tip” when hovering the mouse pointer over the Portal banner (logo) and as the browser window’s title bar.

9. **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.

10. **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 color are displayed. The color used is the same as for active tabs and the active area (see the section "Default Appearance" on page 353).

11. **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.

12. **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`**

13. **Specify whether to install JRE automatically on the client machine or not when Avaya Endpoint Access Control Agent fails due to not finding JRE on client's machine.**

14. **Specify whether to use RSA soft token to Autofill passcode/autocode information or not.**

15. **Specify whether to add site to pop unblock list or not.**

16. **Specify whether to display system information and bandwidth test tool for novice user.**

17. **Specify whether to allow automatic addition of trusted zone.**

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

White-List Settings

One of the fundamental features of the Avaya VPN Gateway product is the act of rewriting HTTP requests to HTTPS. When the remote user enters a URL (e.g. `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 Avaya VPN Gateway. 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 Avaya VPN Gateway.

If unqualified domain names are used (e.g. `inside` instead of `inside.example.com`) the request is always rewritten, even if the domain is not included in the whitelist.

A typical usage would be to specify your intranet domains in the whitelist. The result would 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. **Log on to the BBI as administrator user.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN name from the Name list.**

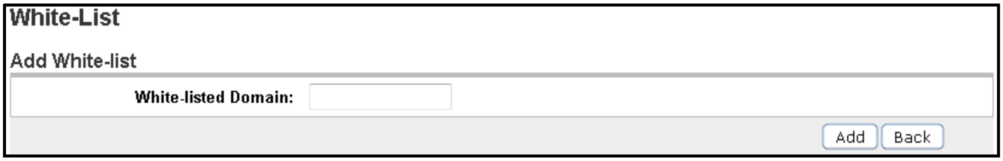
   The VPN Summary screen is displayed.
5. **Under Settings, select Portal.**

   The Portal General setting screen is displayed
6. **Click on White-List tab.**

   The White-List form is displayed.
7. **Under White-list Settings, in the URL Rewrite White-list list box, select `on`.**

   This allows you to specify which URLs are to be rewritten and also configuring the domains which are to be rewritten.
8. **Click Update.**

9. **Click Add.**



White-List

Add White-list

White-listed Domain:

10. **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 Avaya VPN Gateway rewrite prefix (in boldface as follows):

    `https://vpn.example.com``/http/www.example.com`

11. **Click Add.**

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

Black-List Settings

Using the Black-List form (VPN Gateways>VPN #>Portal Display>Black-List), you can specify a list of domains to which requests should *not* be rewritten (compare to the whitelist on the previous page).

The system first checks the whitelist to see if the request matches a domain listed there. It then continues to check the blacklist to see if the request matches a blacklisted 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.

1. **Log on to the BBI as administrator user.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN name from the Name list.**

   The VPN Summary screen is displayed.

5. **Under Settings, select Portal.**

   The Portal General setting screen is displayed

6. **Click on Black-List tab.**

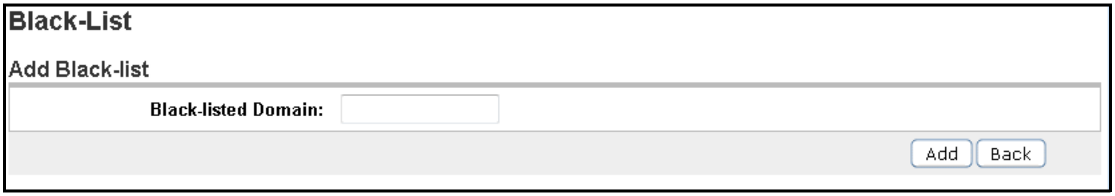
The White-List form is displayed.

7. **Under Black-list Settings, in the URL Rewrite White-list list box, select on.**

   This allows you to specify which URLs are to be rewritten and also configuring the domains which are to be rewritten.

8. **Click Update.**

9. **Click Add.**



Black-List

Add Black-list

Black-listed Domain:

10. **Specify the domain to be added in the black-list domains list.**

11. **Click Add.**

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

Change the Presentation

To change the Portal’s look and feel, proceed as follows:

1. **Log on to the BBI as administrator user.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN name from the Name list.**

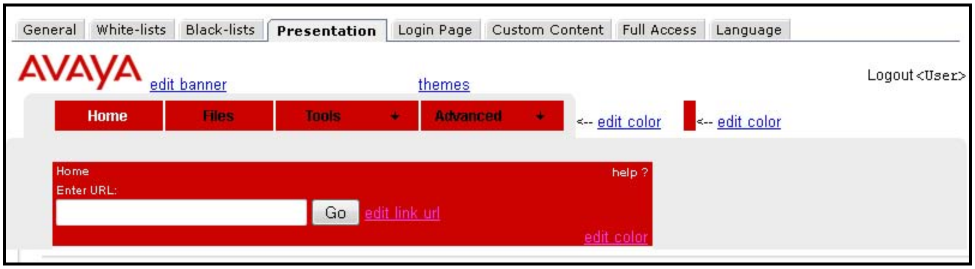
   The VPN Summary screen is displayed.

5. **Under Settings, select Portal.**

   The Portal General setting screen is displayed

6. **Select Presentation.**

A graphic representation of the Portal is displayed.

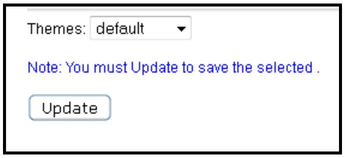


7. **In the VPN Number list box, select the VPN whose Portal presentation you wish to change.**

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.



Themes: default

Note: You must Update to save the selected .

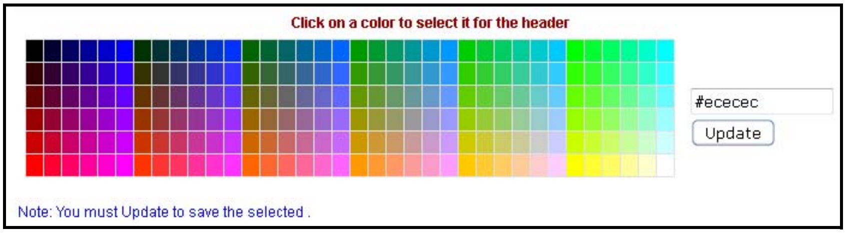
2. **Select the desired theme and click Update.**

   The color theme is applied to the graphic.

   Even though the Portal's individual colors can be changed (see next step), Avaya recommends that you use 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.



Click on a color to select it for the header

#ececec

Update

Note: You must Update to save the selected .

4. **Select the desired color in the map or enter a hexadecimal value corresponding to the color you wish to use.**

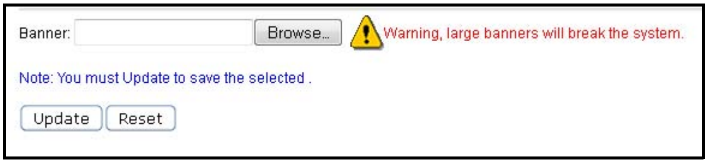
   The hexadecimal value displayed in the field corresponds to the selected color. For a reference to some common colors and their hexadecimal color codes, see the table "Common Colors with Hexadecimal Color Codes." on page 363.

5. **Click Update.**

Change Banner

1. **To change the default banner (logo), click `edit banner`.**

   The Banner field appears under the Portal graphic.



Banner: Browse... Warning, large banners will break the system.

Note: You must Update to save the selected .

Update Reset

   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

Use these instructions to replace the default text that reads "This is a configurable text...".

1. **Edit the static text by clicking `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. TIf 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.

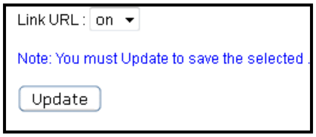
5. **Apply the changes.**

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 is displayed:

    Link URL : on

    Note: You must Update to save the selected

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 10-1 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. **Log on to the BBI as administrator user.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN name from the Name list.**

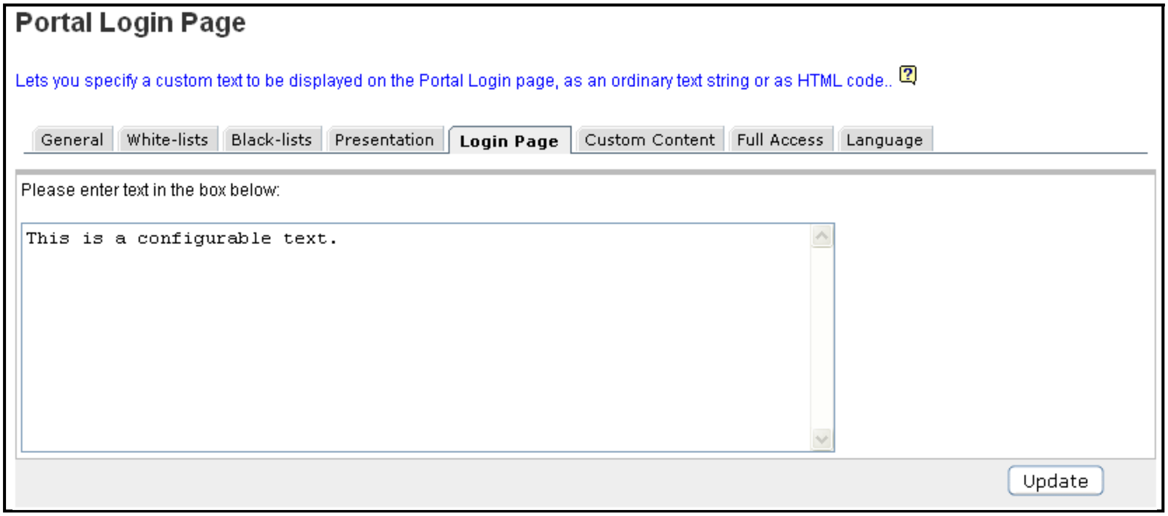
   The VPN Summary screen is displayed.

5. **Under Settings, select Portal.**

   The Portal General setting screen is displayed

6. **Select Login Page.**

   The Login Page form is displayed.



Portal Login Page

Lets you specify a custom text to be displayed on the Portal Login page, as an ordinary text string or as HTML code..

Please enter text in the box below:

```
This is a configurable text.
```

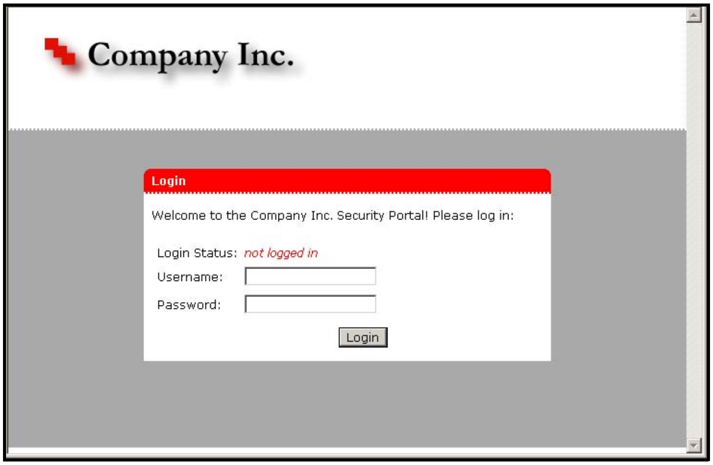
7. **Enter the desired text in the text box and click Update.**

   The text can be entered as an ordinary text string or as HTML code.

8. **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.



Company Inc.

Login

Welcome to the Company Inc. Security Portal! Please log in:

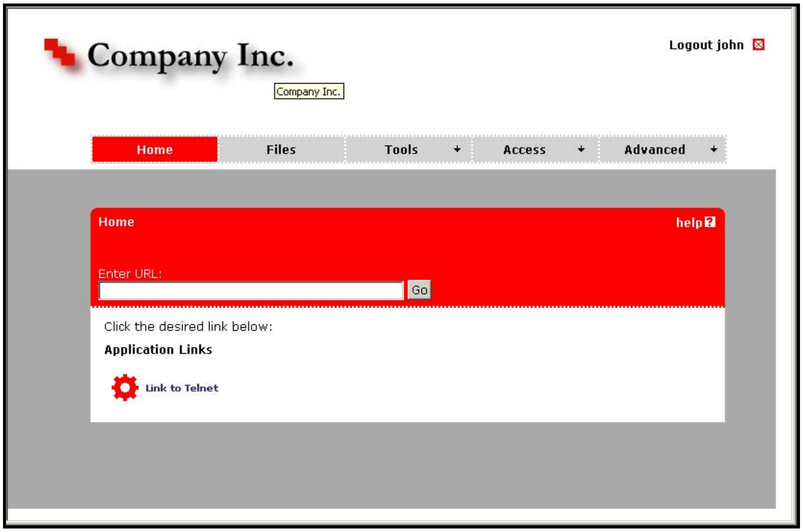
Login Status: *not logged in*

Username:

Password:

Figure 10-2 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.



Company Inc.

Company Inc.

Logout john

Home

Enter URL:

Click the desired link below:

Application Links

Figure 10-3 Portal with New Logo, Colors, Static Text and Company Name

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. **Log on to the BBI as administrator user.**
2. **Click on Config tab.**
3. **In the System tree view, select VPN Gateways.**
4. **Select the VPN name from the Name list.**

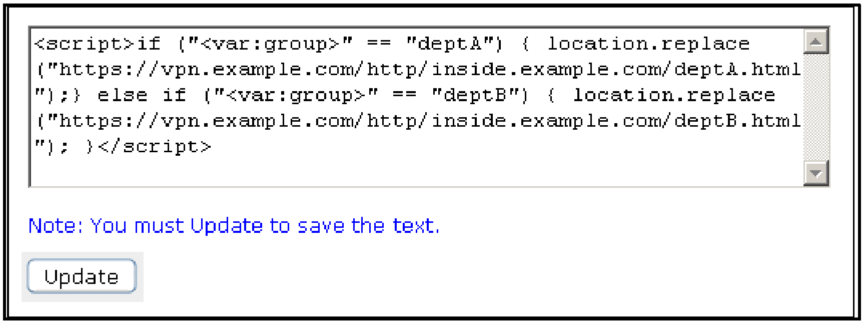
   The VPN Summary screen is displayed.

5. **Select the portal from the settings.**
6. **The Portal General setting screen is displayed.**
7. **Select Presentation.**

   The Portal Presentation form is displayed.

8. **On the Portal graphic, click edit static text.**
9. **A text field is displayed under the Portal graphic.**

10. **Enter a script like the following:**



```
<script>if ("<var:group>" == "deptA") { location.replace
("https://vpn.example.com/http/inside.example.com/deptA.html
");} else if ("<var:group>" == "deptB") { location.replace
("https://vpn.example.com/http/inside.example.com/deptB.html
"); }</script>
```

Note: You must Update to save the text.

In the preceding example, deptA and deptB are group names.

11. **Click Update.**

12. **Apply the changes.**

13. **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 Avaya VPN Gateway 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.

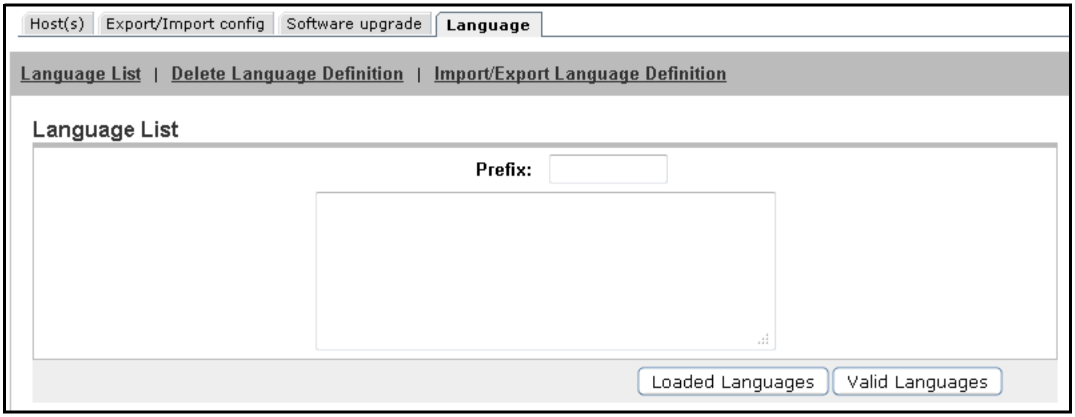
1. **In the System tree view, expand Administration.**

2. **Select Operation.**

The Host(s) screen is displayed.

3. **Select Language.**

The Language form is displayed. Scroll down to Import/Export Language definition.



4. **In the File System specify the desired transfer mode Protocol or Local.**

5. **In the File field, enter a name for the language definition file, e.g. `template.po`.**

6. **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), edit the language definition file and reload it (see "Import Language Definition File" on page 369).

```
#: 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 Avaya VPN Gateway 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.

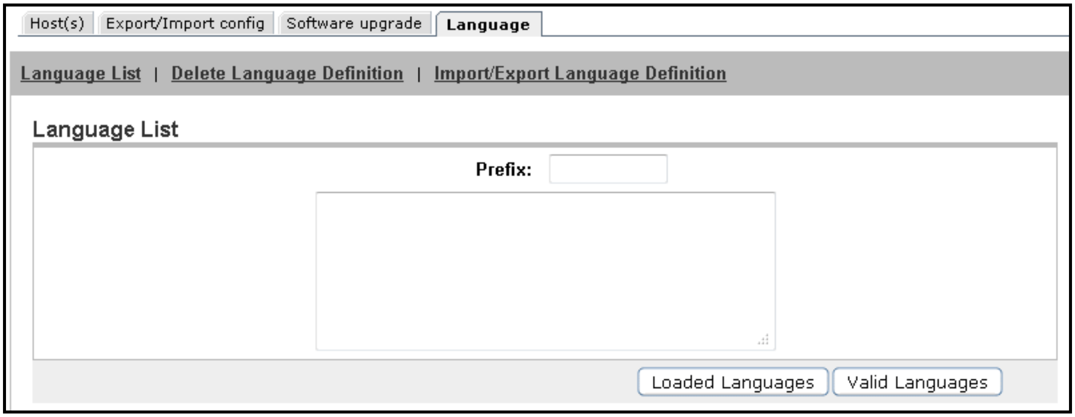
The next step is to import the language definition file your have translated to the Avaya VPN Gateway.

Import Language Definition File

1. **In the System tree view, expand Administration.**
2. **Select Operation.**

   The Host(s) screen is displayed.
3. **Select Language.**

   The Language form is displayed. Scroll down to Import/Export Language definition.



4. **In the File System specify the desired transfer mode Protocol or Local.**
5. **In the File field, enter a name for the language definition file, for example `template.po`.**
6. **Click Import Language.**

   The next step is to translate the language definition file you have exported.

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 e.g. e in the Prefix field before clicking the button.

Configure the Portal to Use New Language

1. **Log on to the BBI as administrator user.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN name from the Name list.**

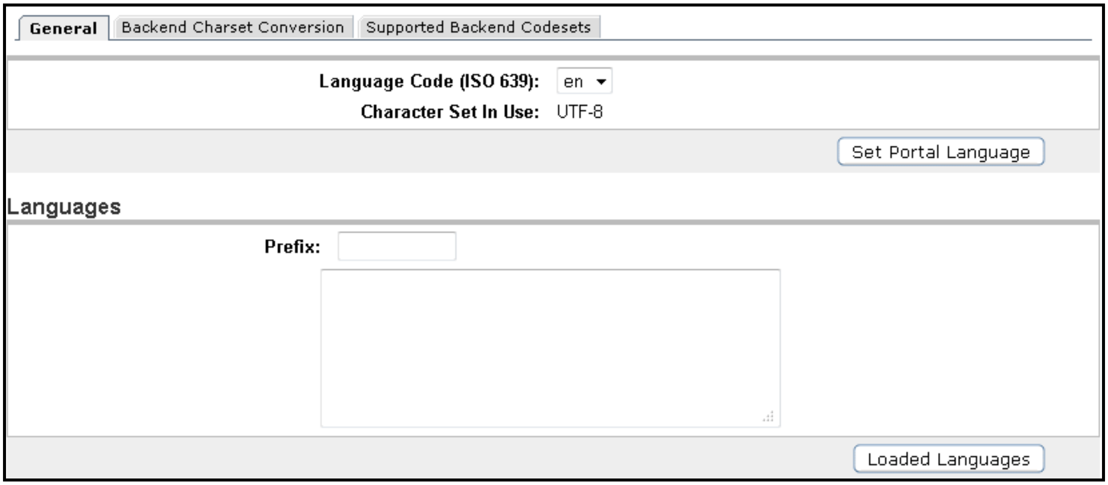
   The VPN Summary screen is displayed.

5. **Select the portal from the settings.**

   The Portal General setting screen is displayed.

6. **Select Language.**

   The Portal Language form is displayed.



Language Code (ISO 639): en
Character Set In Use: UTF-8
Prefix:

7. **In the Language Code list box, select the language code corresponding to the imported language definition file.**

8. **Click Set Portal Language.**

9. **Apply the changes.**

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 Avaya VPN Gateway 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. **Log on to the BBI as administrator user.**

2. **Click on Config tab.**

3. **In the System tree view, select VPN Gateways.**

4. **Select the VPN name from the Name list.**

   The VPN Summary screen is displayed.

5. **Under Settings, select Portal.**

   The Portal General setting screen is displayed.

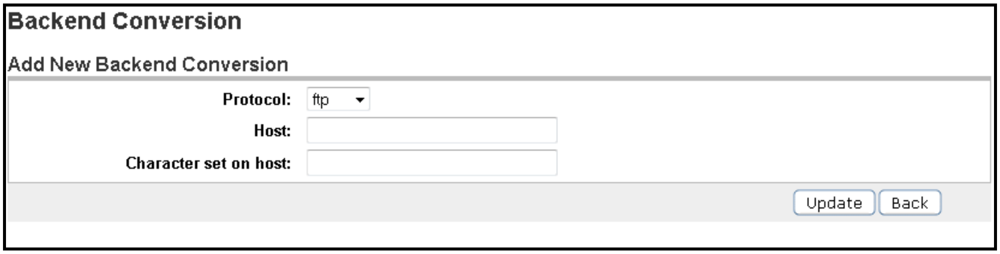
6. **Select Language.**

   The Portal Language form is displayed.

7. **Select Backend Charset Conversion.**

8. **Click Add.**

The Add New Backend Conversion form is displayed.



Backend Conversion

Add New Backend Conversion

Protocol:	ftp
Host:	
Character set on host:	

9. **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.

10. **In the Host field, specify the backend file server's host name or IP address.**

11. **In the Character set on host field, specify the character set to be converted, e.g. ISO-8859-1.**

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

13. **To add another backend conversion entry, repeat Step 4 to Step 12.**

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, e.g. `https://vpn.example.com/content/example.html`. You can also create a Portal link to the content, using the External Website link type (see Chapter 11, "Group Links"). 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 `nortel_cacheable`. Then store the content in this directory before zipping the files (sub-directories may exist).

NOTE – File and directory names are case sensitive.

Examples of zip file contents:

- noncacheable_content1.html
- subdir/noncacheable_content2.html
- nortel_cacheable/mycacheable_content1.html
- nortel_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.

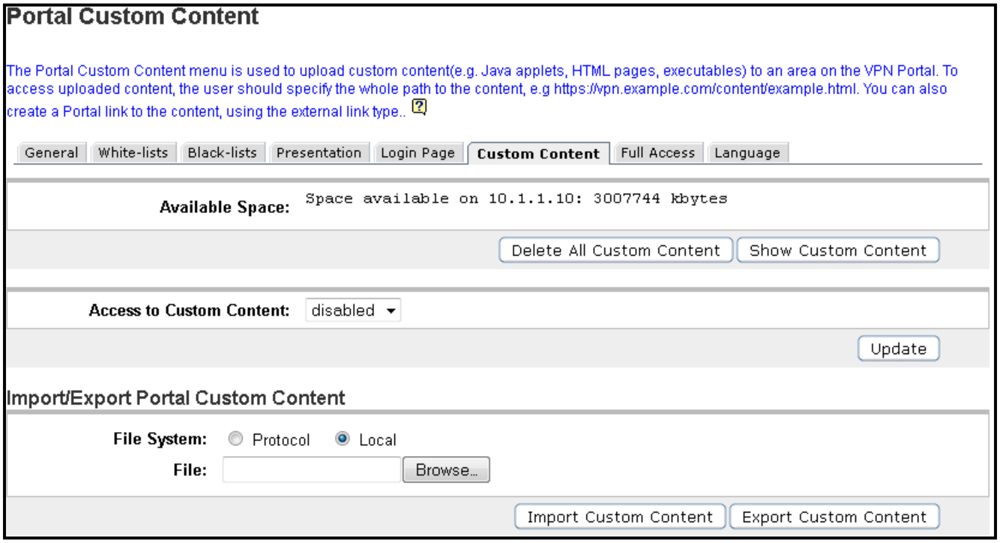
NOTE – A previously imported zip file will be replaced with the new file. If you want to save existing Portal content, first export this content using the Export Custom Content button.

1. **In the System tree view, select VPN Gateways.**
2. **Select the VPN name from the Name list.**

   The VPN Summary screen is displayed.
3. **Under Settings, select Portal.**

   The Portal General setting screen is displayed.
4. **Select Custom Content.**

The Portal Custom Content form is displayed.



Portal Custom Content

The Portal Custom Content menu is used to upload custom content(e.g. 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, e.g https://vpn.example.com/content/example.html. You can also create a Portal link to the content, using the external link type..

Available Space: Space available on 10.1.1.10: 3007744 kbytes

Access to Custom Content: disabled

Import/Export Portal Custom Content

File System: ○ Protocol ● Local

File:

5. **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

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 11
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 (page 378).
- ***FTP***. Gives the user access to folders on an FTP file server (page 381).
- ***External***. Link (direct) to web page. Suitable for external web sites (page 385).
- ***Internal***. Link (secured) to web page. Suitable for internal web pages (page 388).
- ***Iauto***. Automatic login link (secured) to password-protected web page (page 389).
- ***Terminal***. Link to terminal server through Java applet for Telnet or SSH connections (page 395).
- ***HTTP proxy***. Link for accessing web pages through the Avaya VPN Gateway's HTTP Proxy server (page 422).
- ***FTP proxy***. Application tunnel link to a specified FTP server (page 426).
- ***Custom***. Application tunnel link to a custom application server (page 398).
- ***Telnet***. Application tunnel link to terminal server for Telnet connections.
- ***Mail***. Application tunnel link to mail server (for example Outlook Express).
- ***Netdrive***. Application tunnel link for mapping a network drive to an SMB (Windows file share) file server.
- ***WTS***. Application tunnel link to Windows Terminal Server (page 404).
- ***Outlook***. Application tunnel link to Microsoft Exchange server (page 417).
- ***Net Direct***. Portal link used to download and start the Net Direct client (downloadable version of the Avaya VPN Client (page 137).

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 repeatedly for each group. For group-specific links, simply create a linkset that is exclusive for that group.

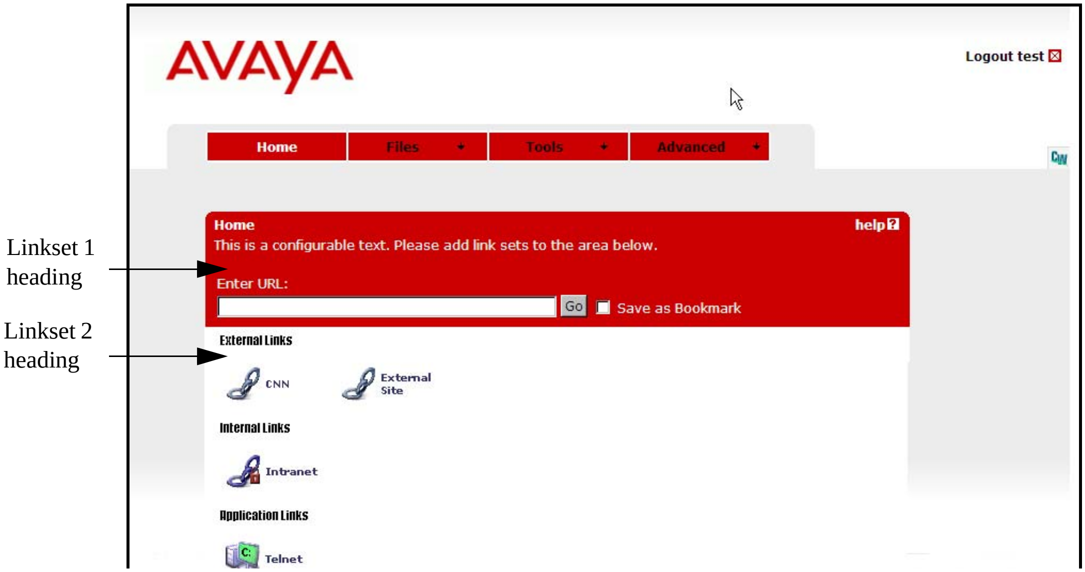
Make sure that access to the resource provided through the link is not contradicted by any access rules that apply to the group(s) in which the remote user is a member.

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.



Home

This is a configurable text. Please add link sets to the area below.

Enter URL:

Autorun Support

With autorun support enabled, all links contained 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

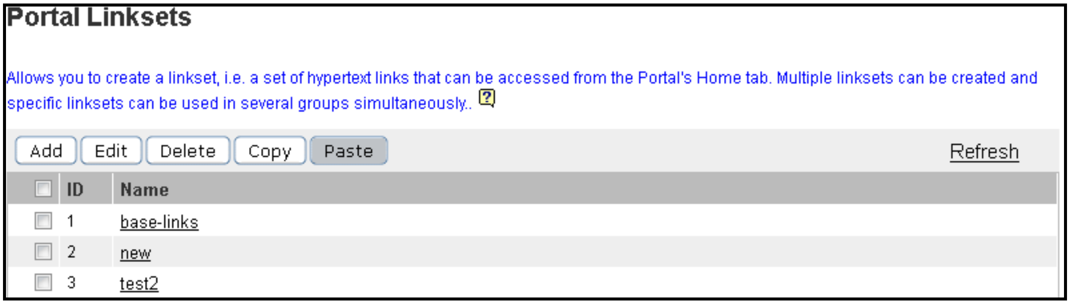
In this example we will create a specific linkset for file server access. The linkset should include two links, one for access to an SMB (Windows file share) file server and one for access to an FTP server.

1. **Log on as system admin.**
2. **Click on Config tab.**
3. **In the system tree view, select VPN Gateways.**

   VPN Gateways screen is displayed.
4. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.
5. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.



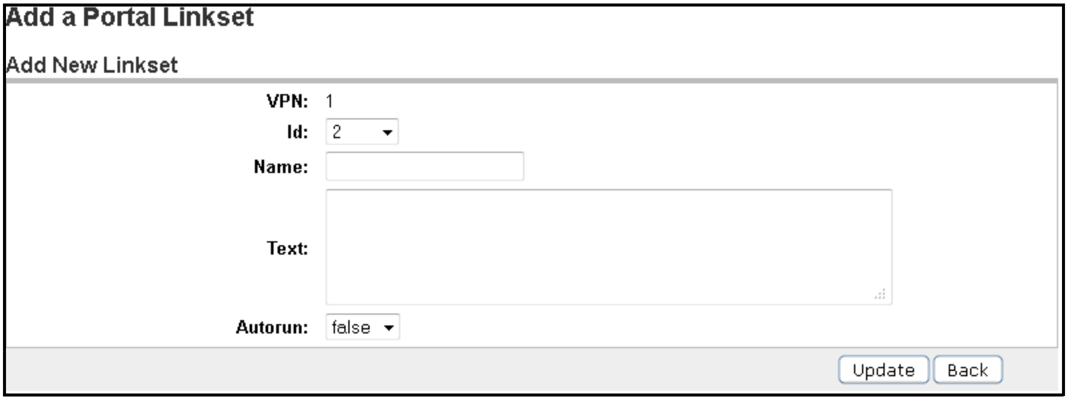
Portal Linksets

Allows you to create a linkset, i.e. a set of hypertext links that can be accessed from the Portal's Home tab. Multiple linksets can be created and specific linksets can be used in several groups simultaneously.

□	ID	Name
□	1	base-links
□	2	new
□	3	test2

6. **Click Add.**

   Add a Portal Linkset form is displayed.



Add a Portal Linkset

Add New Linkset

VPN: 1

Id: 2

Name:

Text:

Autorun: false

7. **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`.

8. **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.

9. **Click Update.**

10. **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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present go to Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

    Add Portal Links form is displayed.

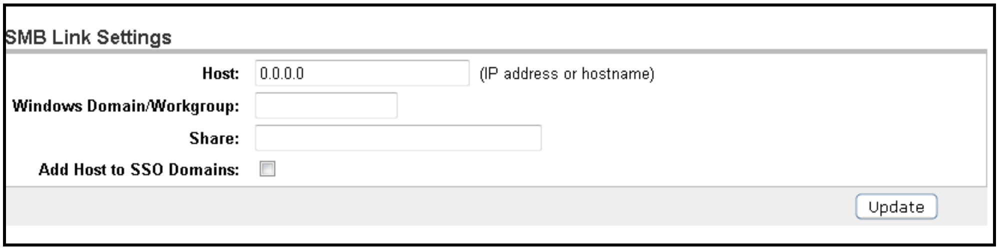
12. **In the Text field, enter the clickable link text to be displayed on the Portal's Home tab.**

    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 SMB Link Settings form is displayed.



SMB Link Settings

Host: 0.0.0.0 (IP address or hostname)

Windows Domain/Workgroup:

Share:

Add Host to SSO Domains: □

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, e.g. `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>VPN #>SSO Domains and Headers.**

    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, e.g.: **`user:password@smb.example.com`**.

19. **Click Update and 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present go to Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

Portal Links form is displayed.

11. **Click Add.**

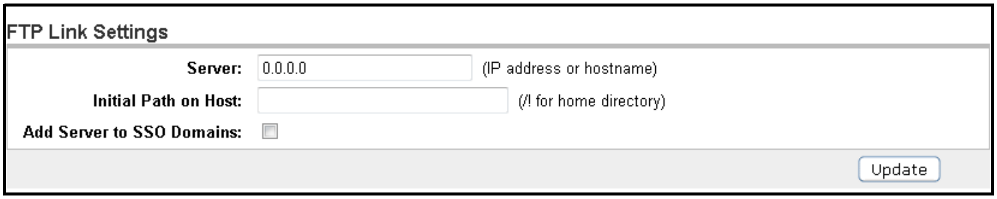
12. **In the Text field, enter the clickable text to appear on the Portal's Home tab.**

    In this example, enter the text `Link to FTP file server`.

13. **In the Link Type list box, select FTP.**

14. **Click Continue.**

    The FTP Link Settings form is displayed.



FTP Link Settings

Server:	0.0.0.0	(IP address or hostname)
Initial Path on Host:		(/! for home directory)
Add Server to SSO Domains:	□	

15. **Under FTP Link Settings, 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 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>VPN #>SSO Domains and Headers**.

    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, e.g.: **`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.**

19. **Apply the changes.**

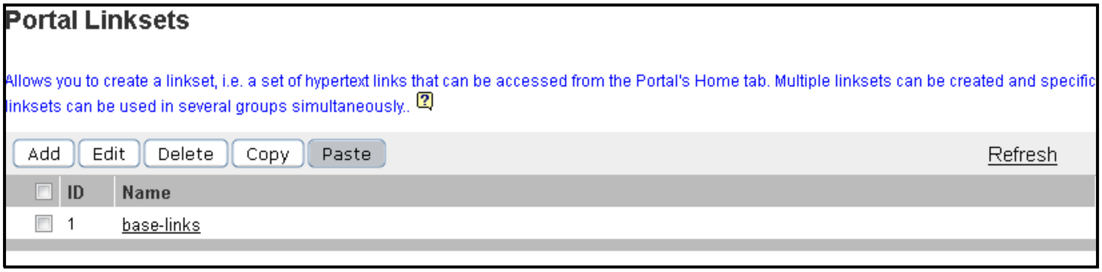
View Created Links in BBI

1. **To view the new links, select VPN Gateways in system tree view.**

2. **Under Settings, click on Link Sets.**

   The links we have just created are displayed in the order they will be displayed on the Portal's

   Home tab.



Portal Linksets

Allows you to create a linkset, i.e. a set of hypertext links that can be accessed from the Portal's Home tab. Multiple linksets can be created and specific linksets can be used in several groups simultaneously..

□	ID	Name
□	1	base-links

3. **Apply the changes.**

Map the Linkset to a Group

Linkset 1 now includes two links, one link to an SMB file server and one link to an FTP file server. For a group member to be able to access the links, the linkset must be mapped to the desired groups.

1. **In the system tree view, select VPN Gateways.**

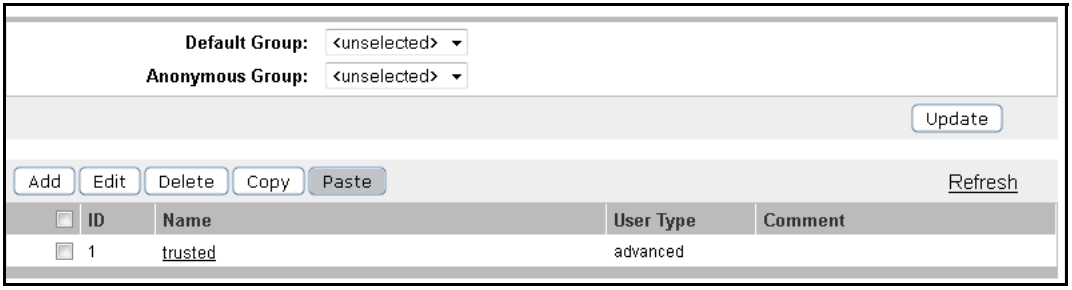
2. **VPN Gateways screen is displayed.**

3. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

4. **Under Settings, click on Groups.**

Groups form is displayed.



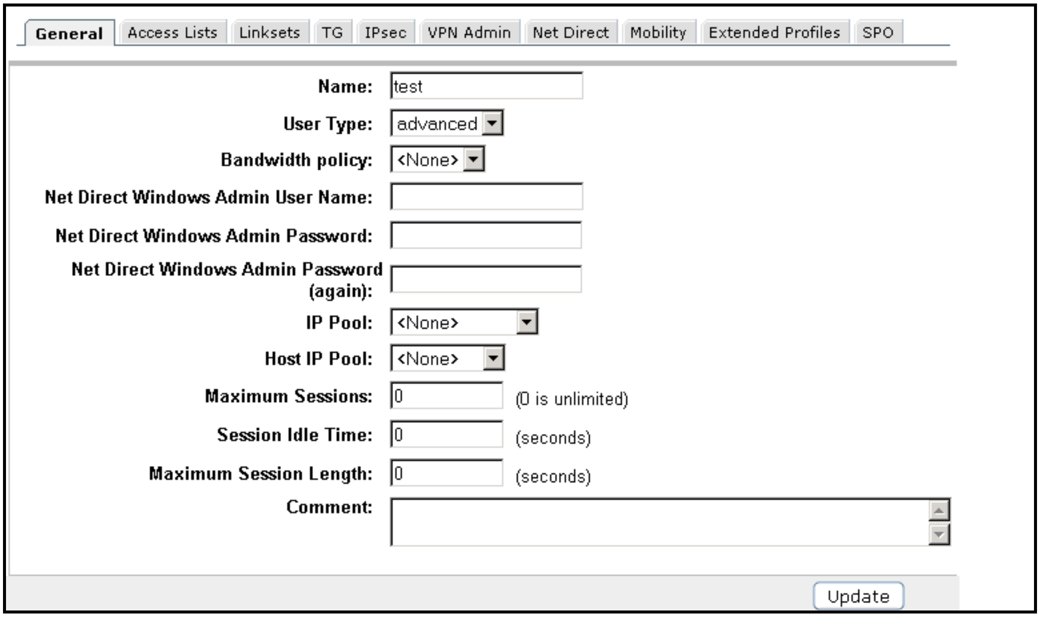
Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

5. **Click on the group name.**

Modify a Group form is displayed.



Name: test

User Type: advanced

Bandwidth policy: <None>

Net Direct Windows Admin User Name:

Net Direct Windows Admin Password:

Net Direct Windows Admin Password (again):

IP Pool: <None>

Host IP Pool: <None>

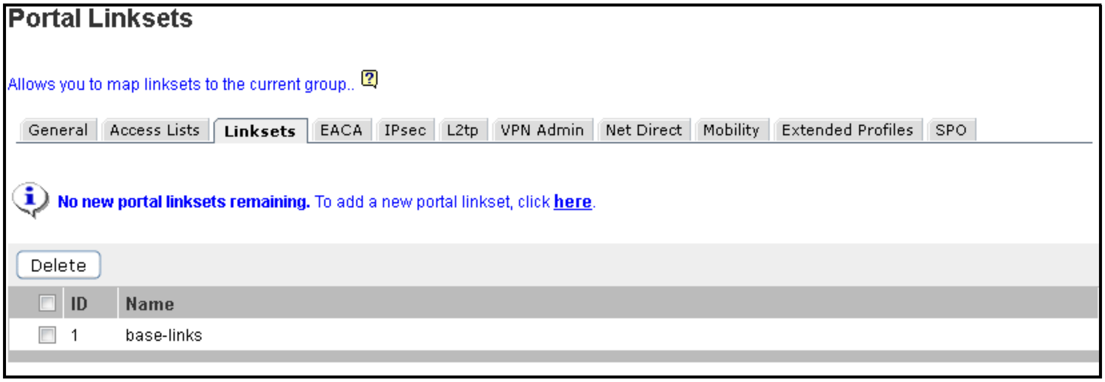
Maximum Sessions: 0 (0 is unlimited)

Session Idle Time: 0 (seconds)

Maximum Session Length: 0 (seconds)

Comment:

6. **Click on Linksets tab in Modify a Group form.**



Portal Linksets

Allows you to map linksets to the current group..

No new portal linksets remaining. To add a new portal linkset, click **here**.

□	ID	Name
□	1	base-links

7. **In the Portal Linksets list box, select the linkset you wish to map to the group, i.e Link to Home from Shared Folder.**

8. **Click Add.**

9. **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, refer to the previous section, "Create a Linkset for File Server Access" on page 377.

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 Avaya VPN Gateway rewrite prefix (compare to "Example 4: Secured Link to Web Page (Internal)" on page 388).

1. **In the system tree view, select VPN Gateways.**

   VPN Gateways screen is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present goto Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

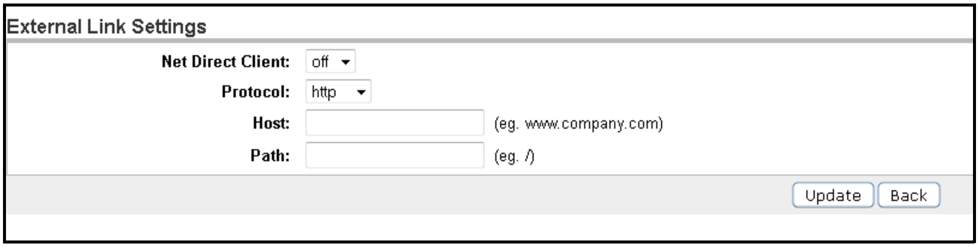
12. **In the Text field, enter the clickable link text to appear on the Portal's Home tab.**

    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 External Link Settings form is displayed.



External Link Settings

Net Direct Client:	off	
Protocol:	http	
Host:		(eg. www.company.com)
Path:		(eg. /)

15. **Under External Link Settings, in the Protocol list box, select the desired access protocol, `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 Avaya 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present goto Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

    The Add Portal Links form is displayed.

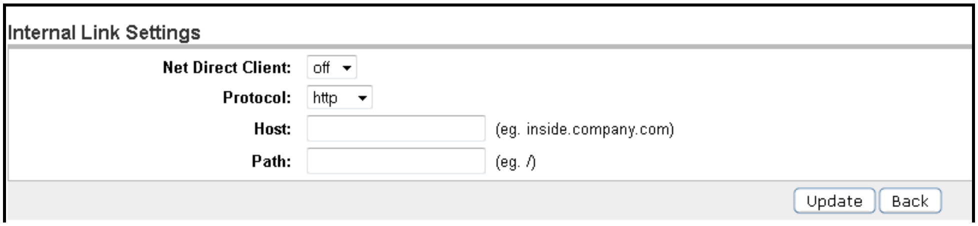
12. **In the Text field, enter the clickable link text to appear on the Portal’s Home tab.**

    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 Internal Link Settings form is displayed.



Internal Link Settings

Net Direct Client: off

Protocol: http

Host: (eg. inside.company.com)

Path: (eg. /)

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 5a: Automatic Login Link Secured by the Avaya VPN Gateway (lauto)

This example shows how to create an automatic login link to a password-protected web page. The HTTP request is directed to the Avaya VPN Gateway, 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 Avaya VPN Gateway 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 414".

1. **In the system tree view, select VPN Gateways.**

   VPN Gateways screen is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present goto Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

Portal Links form is displayed.

11. **Click Add.**

    The Add Portal Links form is displayed.

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 `Secure auto-logon link to web page`.

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. **Under Iauto Link Settings, in the Login URL field, enter the URL to the password-protected web page.**

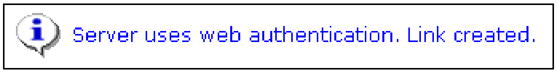
    Example 1 (HTTP-based authentication):
    `http://inside.example.com/login/login.htm`

    Example 2 (form-based authentication):
    `http://inside.example.com/login/login.asp`

16. **Click Submit.**

    The Avaya VPN Gateway 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:

    Server uses web authentication. Link created.

    A link to the web page has been created. When the user clicks the link on the Portal’s Home tab, the Avaya VPN Gateway 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 Avaya VPN Gateway 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>VPN #>Link Sets>Portal 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 is displayed 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>VPN #>Authentication>(Method)>General**).

17. **Click Submit.**

    If needed, the values that you have specified can later be edited under Internal Auto Mapping (**VPN Gateways>VPN #>Link Sets>Portal 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 *User's Guide*.

18. **Apply the changes.**

Example 5b: 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present go to Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

    The Add Portal Links form is displayed.

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?Client-
    Detection=On
    ```

    Example 2 (Web Interface 3.0):

    ```
    http://citrix.example.com/Citrix/MetaFrame/default/login.aspx?Client-
    Detection=On
    ```

16. **Click Submit.**

    The Avaya VPN Gateway 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 is displayed 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>VPN #>Authentication>(Method)>General**).

17. **Click Submit.**

    If needed, the values that you have specified can later be edited under Internal Auto Mapping (**VPN Gateways>VPN #>Link Sets>Portal 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 *User's Guide*.

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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present goto Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

The Add Portal Links form is displayed.

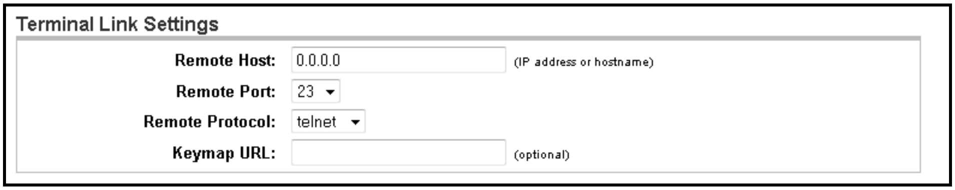
12. **In the Text field, enter the clickable link text to appear on the Portal's Home tab.**

    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.**

    Terminal Link Settings form is displayed.



Terminal Link Settings

Remote Host:	0.0.0.0	(IP address or hostname)
Remote Port:	23	
Remote Protocol:	telnet	
Keymap URL:		(optional)

15. **Under Terminal Link Settings, in the Remote Host field, enter the IP address or host name of the remote terminal server, e.g. `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.

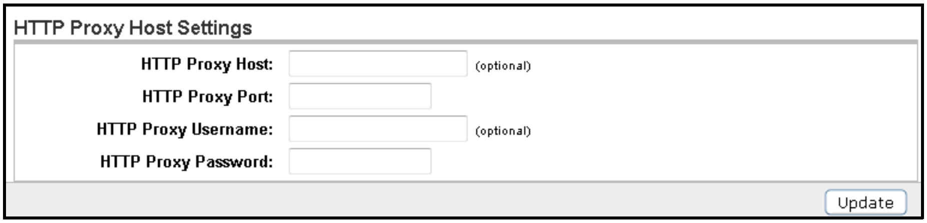
18. **In the Keymap URL field (optional), enter the path to a keyboard mapping file.**

    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, e.g. `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.**



HTTP Proxy Host Settings

HTTP Proxy Host:		(optional)
HTTP Proxy Port:		
HTTP Proxy Username:		(optional)
HTTP Proxy Password:		

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 Avaya 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 Avaya VPN Gateway, unless Internet Explorer has been configured to use a proxy. In this case this proxy server is used.

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, e.g. 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 the section "Port Forwarder API" on page 422), 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present goto Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

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.**

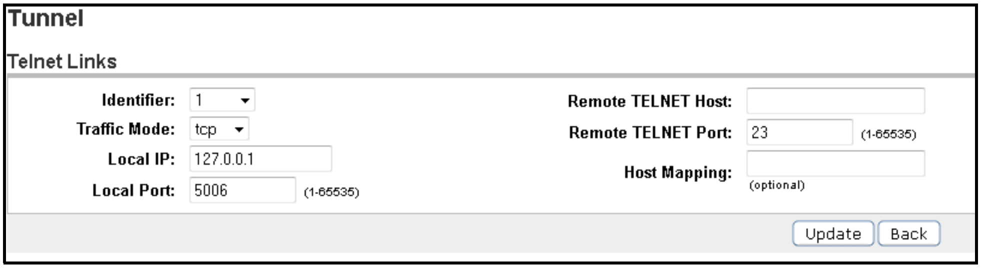
14. **Click Continue.**

15. **Click on Tunnel tab.**

    The Tunnel form is displayed.

16. **Click Add.**

The Custom Links form is displayed.



Tunnel

Telnet Links

Identifier:	1	Remote TELNET Host:	
Traffic Mode:	tcp	Remote TELNET Port:	23 (1-65535)
Local IP:	127.0.0.1	Host Mapping:	(optional)
Local Port:	5006 (1-65535)		

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 Avaya VPN Gateway.

NOTE – Mac OS X uses 127.0.0.1 by default. To use loopback address other than 127.0.0.1, Mac user must configure the loopback alias manually.

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 Avaya 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 `telnet.example.com` is specified as host.

21. **In the Remote Destination Port field, enter the destination port.**

    The destination port number used 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 e.g. 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 Step 28). 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 would 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, e.g. **`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 Step 28). If **`browser`** is entered as executable, the user’s default browser will be started.

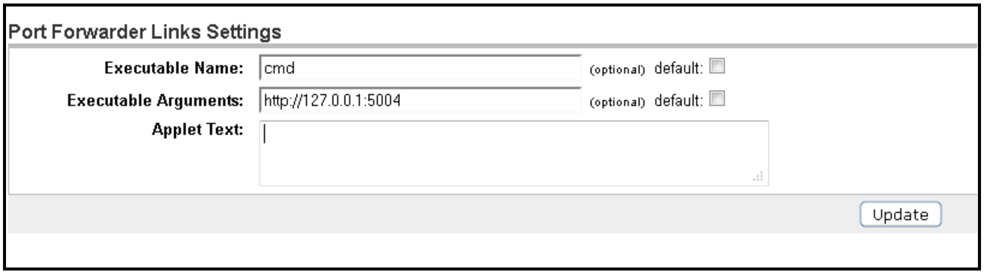
NOTE – The Avaya VPN Gateway must be able to find the executable either through the PATH variable or in the registry (on Windows clients), that is, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths. To make sure the program is found, the complete path to the executable can also be 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, e.g. `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 Step 18.



Port Forwarder Links Settings

Executable Name:	cmd	(optional) default: □
Executable Arguments:	http://127.0.0.1:5004	(optional) default: □
Applet Text:		

28. **In the Applet Text field, enter a custom text (e.g. 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 (e.g. by using the specified host alias).

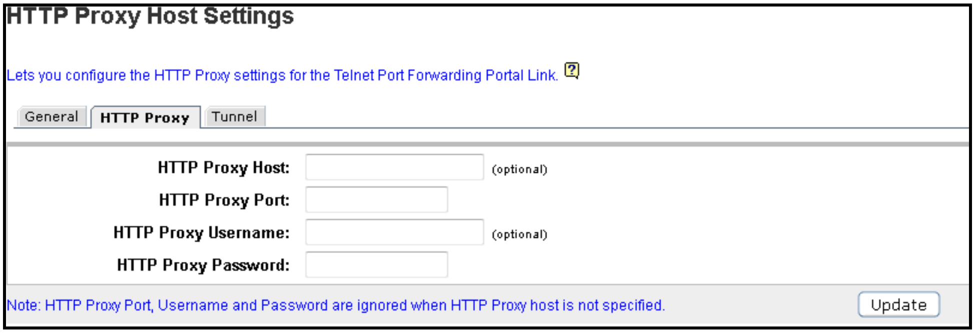
If no custom text is entered, a standard text is displayed in the **Info** part of the Java applet window. Following is an example of a Java applet *standard* text:

```
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 is displayed.



HTTP Proxy Host Settings

Lets you configure the HTTP Proxy settings for the Telnet Port Forwarding Portal Link.

HTTP Proxy Host:	(optional)
HTTP Proxy Port:	
HTTP Proxy Username:	(optional)
HTTP Proxy Password:	

Note: HTTP Proxy Port, Username and Password are ignored when HTTP Proxy host is not specified.

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 Avaya 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 Avaya VPN Gateway, 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 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.

NOTE – If you expect the connection to include more than 15 minutes of inactivity, increase the Client TCP Keep Alive Timeout value (under **VPN Gateways>VPN # >TCP**).

Create a Linkset for Windows Terminal Server

In this example we will create a specific linkset for Windows Terminal Server. .

1. **In the system tree view, select VPN Gateways.**

   VPN Gateways screen is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present go to Step 10.**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

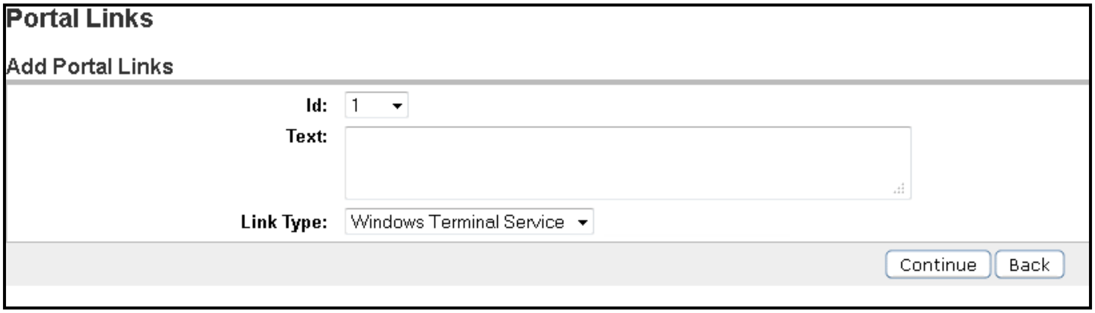
9. **Apply the changes.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**



Portal Links

Add Portal Links

Id: 1

Text:

Link Type: Windows Terminal Service

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`.

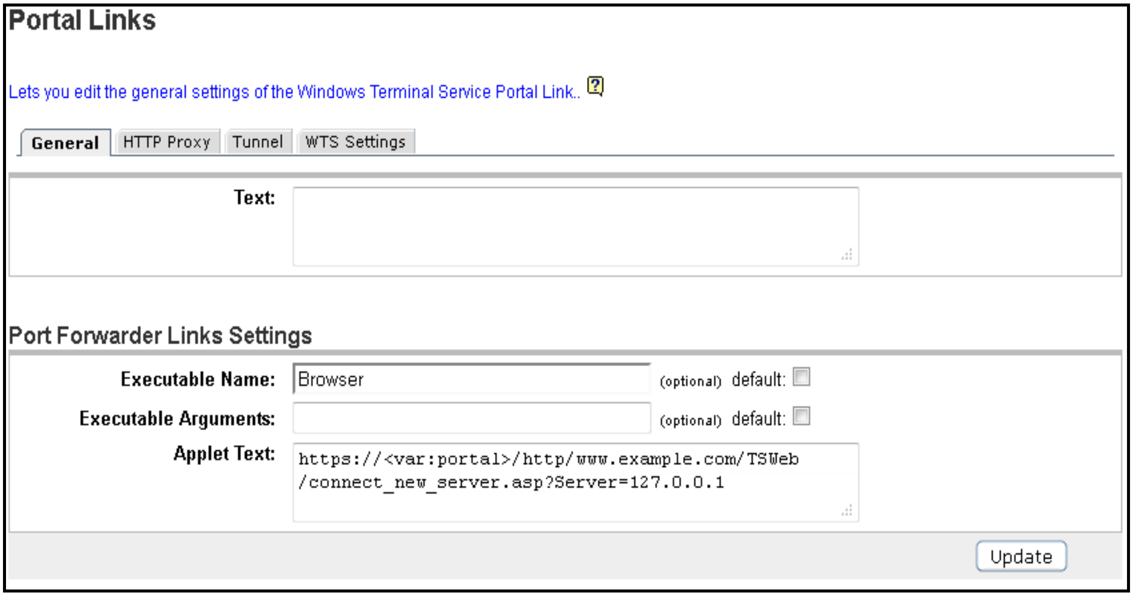
13. **In the Link Type list box, select the desired link type, that is, Windows Terminal Server.**

14. **Click Continue.**

15. **From the General tab,specify in the Text box the clickable link text to appear on the Portal's Home tab.**

16. **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`**



Portal Links

Lets you edit the general settings of the Windows Terminal Service Portal Link..

Text:

Port Forwarder Links Settings

Executable Name: Browser (optional) default: □

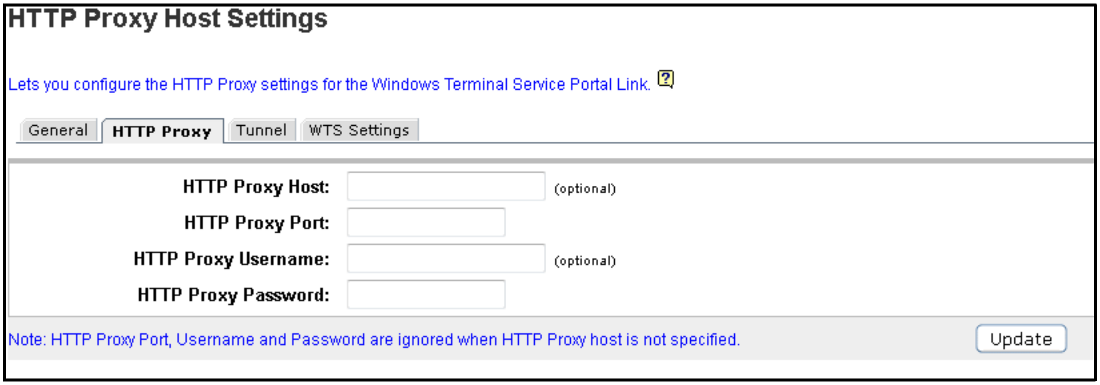
Executable Arguments: (optional) default: □

Applet Text:
```
https://<var:portal>/http/www.example.com/TSWeb
/connect_new_server.asp?Server=127.0.0.1
```

17. **Click Update.**

NOTE – Mac OS X uses 127.0.0.1 by default. To use loopback address other than 127.0.0.1, Mac user must configure the loopback alias manually.

18. **Click on the HTTP Proxy tab.**



HTTP Proxy Host Settings

Lets you configure the HTTP Proxy settings for the Windows Terminal Service Portal Link.

HTTP Proxy Host: (optional)

HTTP Proxy Port:

HTTP Proxy Username: (optional)

HTTP Proxy Password:

Note: HTTP Proxy Port, Username and Password are ignored when HTTP Proxy host is not specified.

19. **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 Avaya 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 Avaya VPN Gateway, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.

20. **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.**

21. **Click Update.**

22. **Click on the Tunnel tab.**

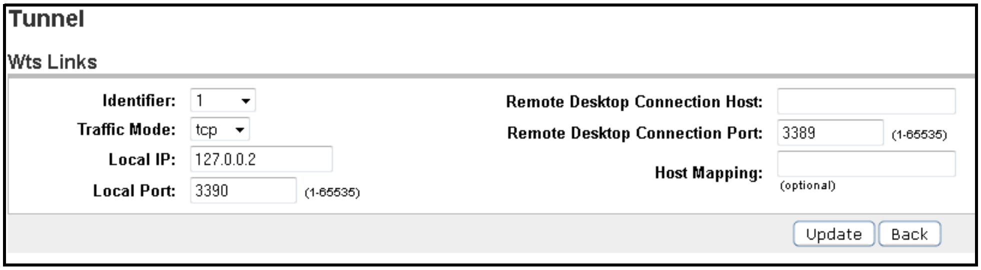
    The Tunnel form is displayed.

23. **Click Add.**

    The WTS Links form is displayed.

24. **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 127.0.0.2 on port 3390, which is the application-specific port number for Windows Terminal Server sessions.



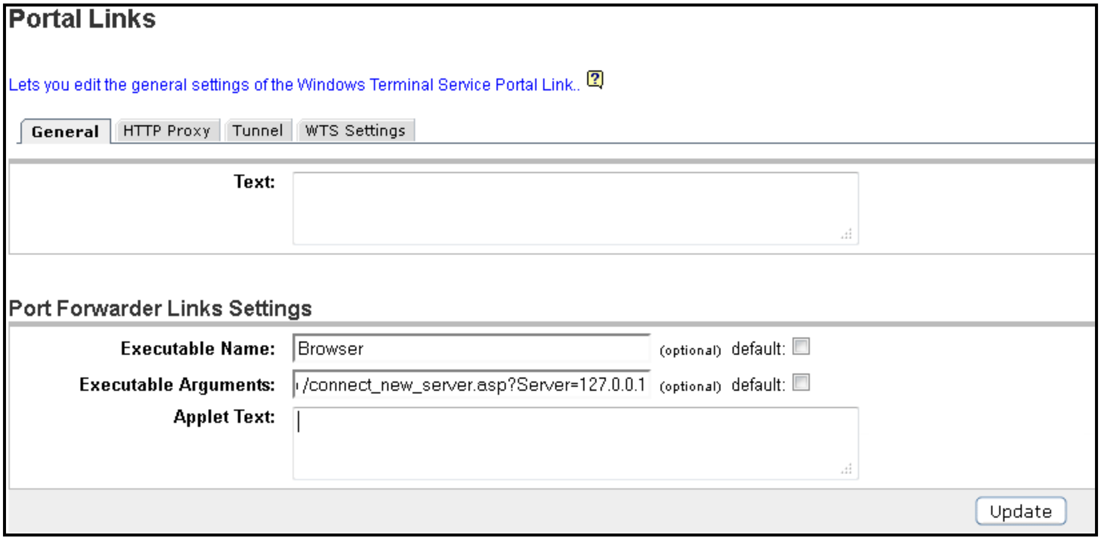
Tunnel

Wts Links

Identifier:	1	Remote Desktop Connection Host:	
Traffic Mode:	tcp	Remote Desktop Connection Port:	3389 (1-65535)
Local IP:	127.0.0.2	Host Mapping:	(optional)
Local Port:	3390 (1-65535)		

25. **Click Update.**

26. Click on the WTS Settings tab.



Portal Links

Lets you edit the general settings of the Windows Terminal Service Portal Link..

Text:

Port Forwarder Links Settings

Executable Name: Browser (optional) default: □

Executable Arguments: /connect_new_server.asp?Server=127.0.0.1 (optional) default: □

Applet Text:

Use the following parameters when configuring WTS settings:

Table 1 WTS settings

Parameter	Description
Application Path	Enter the path for the application.for which you are creating the WTS session.
Working Directory	Enter the working directory of the application.
Domain Name	Enter the domain name used by the application.
KeyMap URL	URL to the custom KeyMap file.
Screen Size	Screen size for the WTS session. Possible values are 'Full Screen', '800x600', '1024x768', '1152x864', '1280x720', '1280x768', '1280x800', '1280x960', '1280x1024', '1360x768', '1600x900', '1600x1200', '1680x1050' and '1920x1080'. Default is '800x600'.
Colordepth	Color depth for the WTS session. Possible values are ‘8 bit’, ‘15 bit’, ‘16 bit’, ‘24 bit’ and ‘32 bit (True Color)’. Default value is ‘16 bit’.

Table 1 WTS settings

Parameter	Description
Map Local Drives	Select whether local drives are mapped in the WTS session as network drives. Possible values are ‘on’ and ‘off’. Default is ‘off’.
Connect Local Printers	Select whether local printers are available in the WTS session. Possible values are ‘on’ and ‘off’, Default is ‘off’. This functionality is not available for the java RDP client and will be ignored in that case.
Hide Port Forwarder Window	Whether to hide the port forwarder window or not. Possible values are ‘on’ and ‘off’. Default value is ‘on’ which means port forwarder is not visible.
Set Java RDP As Default Client	Set Java RDP As Default Client: Set Java as Default citrix client.
Enable Single Sign On	Select whether to automatically sign in the user into the WTS session using the credentials used to login to the portal.
Enable Clipboard Redirection	This commands lets you enable or disable the clipboard redirection.

27. **Click Update.**

28. **Apply the changes.**

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, Avaya recommends 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present go to Step 10.**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

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. **Click on Tunnel tab.**

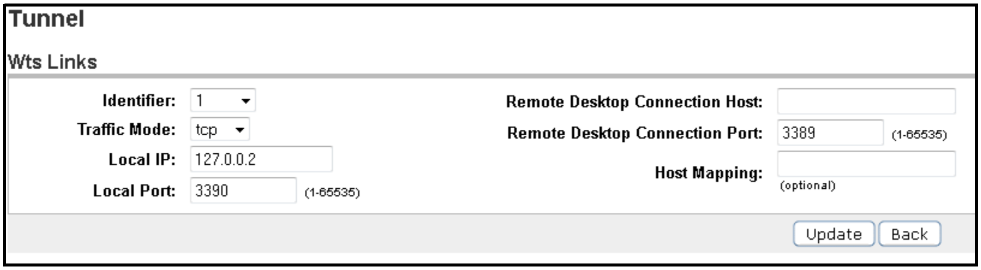
    The Tunnel form is displayed.

16. **Click Add.**

    The WTS Links form is displayed.

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 127.0.0.2 on port 3390, which is the application-specific port number for Windows Terminal Server sessions.



Tunnel

Wts Links

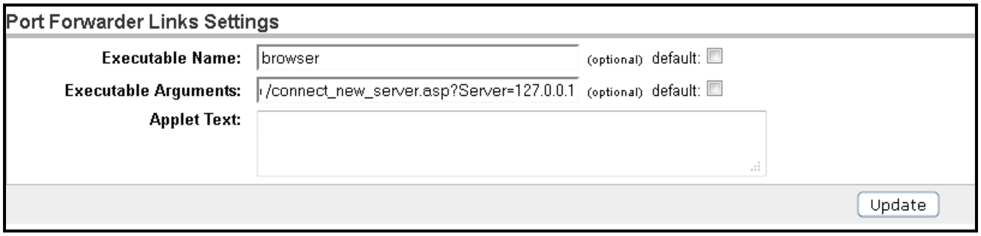
Identifier:	1	Remote Desktop Connection Host:	
Traffic Mode:	tcp	Remote Desktop Connection Port:	3389 (1-65535)
Local IP:	127.0.0.2	Host Mapping:	(optional)
Local Port:	3390 (1-65535)		

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.



Port Forwarder Links Settings

Executable Name: browser (optional) default: □

Executable Arguments: /connect_new_server.asp?Server=127.0.0.1 (optional) default: □

Applet Text:

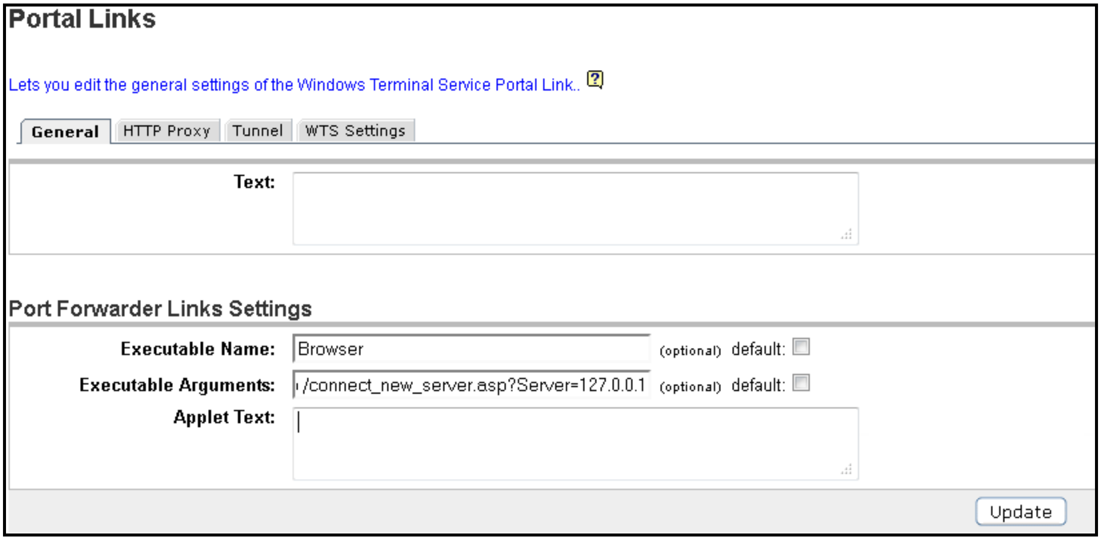
The full argument in the Executable Arguments field reads:
`https://<var:portal>/http/www.example.com/TSWeb /connect_new_server.asp?Server=127.0.0.1`

21. **Click Update.**

    For more detailed descriptions of each field, see example 7a on page 398.

22. **Apply the changes.**

23. **Click on WTS settings tab.**



Portal Links

Lets you edit the general settings of the Windows Terminal Service Portal Link..

Text:

Port Forwarder Links Settings

Executable Name: Browser (optional) default: □

Executable Arguments: /connect_new_server.asp?Server=127.0.0.1 (optional) default: □

Applet Text:

Use the following parameters when configuring WTS settings

Table 2 WTS settings

Parameter	Description
Application Path	Enter the path for the application.for which you are creating the WTS session.
Working Directory	Enter the working directory of the application.
Domain Name	Enter the domain name used by the application.
KeyMap URL	URL to the custom KeyMap file.
Screen Size	Screen size for the WTS session. Possible values are 'Full Screen', '800x600', '1024x768', '1152x864', '1280x720', '1280x768', '1280x800', '1280x960', '1280x1024', '1360x768', '1600x900', '1600x1200', '1680x1050' and '1920x1080'. Default is '800x600'.
Colordepth	Color depth for the WTS session. Possible values are ‘8 bit’, ‘15 bit’, ‘16 bit’, ‘24 bit’ and ‘32 bit (True Color)’. Default value is ‘16 bit’.
Map Local Drives	Select whether local drives are mapped in the WTS session as network drives. Possible values are ‘on’ and ‘off’. Default is ‘off’.
Connect Local Printers	Select whether local printers are available in the WTS session. Possible values are ‘on’ and ‘off’, Default is ‘off’. This functionality is not available for the java RDP client and will be ignored in that case.
Hide Port Forwarder Window	Whether to hide the port forwarder window or not. Possible values are ‘on’ and ‘off’. Default value is ‘on’ which means port forwarder is not visible.
Set Java RDP As Default Client	Set Java RDP As Default Client: Set Java as Default citrix client.
Enable Single Sign On	Select whether to automatically sign in the user into the WTS session using the credentials used to login to the portal.
Enable Clipboard Redirection	This commands lets you enable or disable the clipboard redirection.

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.

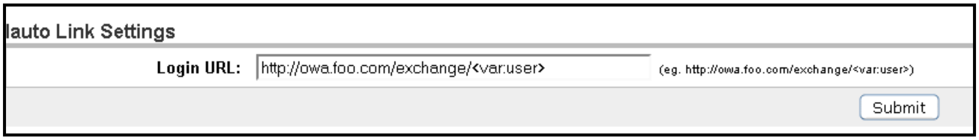
1. **In the system tree view, select VPN Gateways.**
2. **Select the name of the VPN Gateway.**

   VPN Summary screen is displayed.
3. **Under Settings, select Groups.**
4. **Click Add and create a dummy group.**
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.**
9. **Click Add.**

   Add New Linkset form is displayed.
10. **Click Update.**

    The portal linkset name is updated in the database.
11. **Click on the name of the portal linkset.**
12. **Click on Portal Links tab and then click on Add.**
13. **In the Text field, enter the link text iauto for port forwarder.**
14. **In the Link Type list box, select Internal Auto Login URL as link type.**
15. **Click Continue.**

16. **Under Iauto Link Settings, in the Login URL field, enter the URL for authenticating to the Windows Terminal Server.**



Iauto Link Settings

Login URL: http://owa.foo.com/exchange/<var:user> (eg. http://owa.foo.com/exchange/<var:user>)

17. **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.

18. **Enter values for the input fields found on the form. Click Submit.**
19. **In system tree view, select VPN Gateways.**
20. **Select the name of the VPN.**
21. **Under Settings, select Groups.**
22. **Select the name of the group.**
23. **Click on Linksets tab.**
24. **Select the dummy group you created in the portal linkset drop-down list.**
25. **Click Add.**
26. **In the system tree view, select VPN Gateways.**
27. **Select the name of the VPN Gateway.**
28. **Under Settings, select Link Sets.**
29. **Select the name of the portal linkset and click on Portal Link tab.**
30. **Click Add.**

    The Add Portal Links form is displayed.

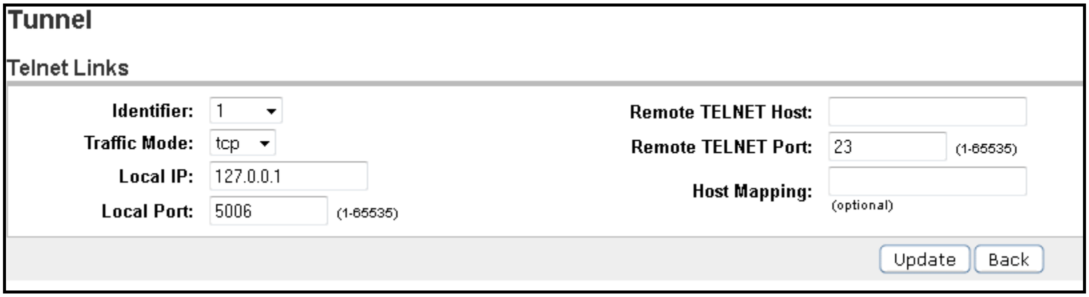
31. **In the Text field, enter the link text to be displayed on the Portal's Home tab.**
32. **Enter the link text WTS auto-login link.**
33. **In the Link Type list box, select Custom Port Forwarding.**
34. **Click Continue.**

Portal Links from in displayed.

35. **Click on Tunnel tab.**

36. **Click Add.**

37. **Enter Tunnel specifics.**



Tunnel

Telnet Links

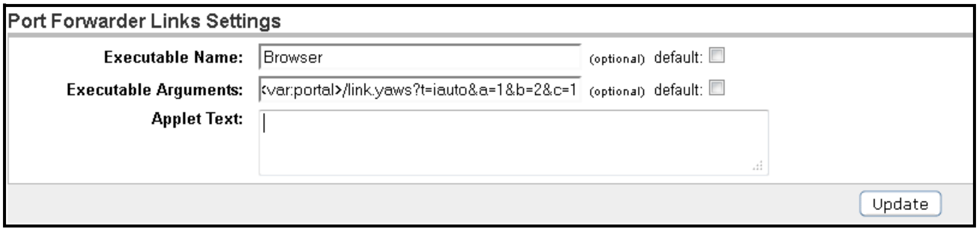
Identifier:	1	Remote TELNET Host:	
Traffic Mode:	tcp	Remote TELNET Port:	23 (1-65535)
Local IP:	127.0.0.1	Host Mapping:	(optional)
Local Port:	5006 (1-65535)		

38. **Click Update.**

39. **In portal Link form, click on General tab.**

40. **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.



Port Forwarder Links Settings

Executable Name:	Browser	(optional) default: ☐
Executable Arguments:	<var:portal>/link.yaws?t=iauto&a=1&b=2&c=1	(optional) default: ☐
Applet Text:		

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.

41. **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>VPN #>DNS**). See Step 36.
- The user must have administrator's rights on their 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 Avaya 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 Avaya 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>VPN #>TCP**).
- To ensure proper operation, specify the DNS name of the portal server in the **DNS Name of VIP field** (under **VPN Gateways>VPN #>General**.

- If a firewall exists between the Avaya 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, e.g. 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present goto Step 10**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

    Add Portal Links form is displayed.

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, select VPN Gateways.**

16. **Select the name of the VPN Gateway.**

17. **Under Settings, select Link Sets.**

18. **Select the name of the portal linkset and click on Portal Link tab.**

19. **Click Add.**

    The Add Portal Links form is displayed.

20. **In the Text field, enter the clickable link text to appear on the Portal's Home tab.**

21. **In this example we will enter the text Link to Outlook.**

22. **In the Link Type list box, select the desired link type, that is, Outlook Port Forwarding.**

23. **Click Continue.**

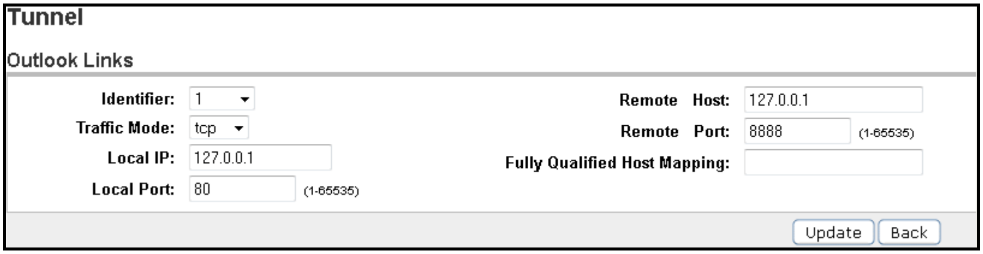
    Portal Links from in displayed.

24. **Click on Tunnel tab.**

25. **Click Add.**

26. **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.



Tunnel

Outlook Links

Identifier: 1

Traffic Mode: tcp

Local IP: 127.0.0.1

Local Port: 80 (1-65535)

Remote Host: 127.0.0.1

Remote Port: 8888 (1-65535)

Fully Qualified Host Mapping:

The host entered in the Fully Qualified Host Mapping field reads `exchange1.example.com`.

27. **Click Update.**

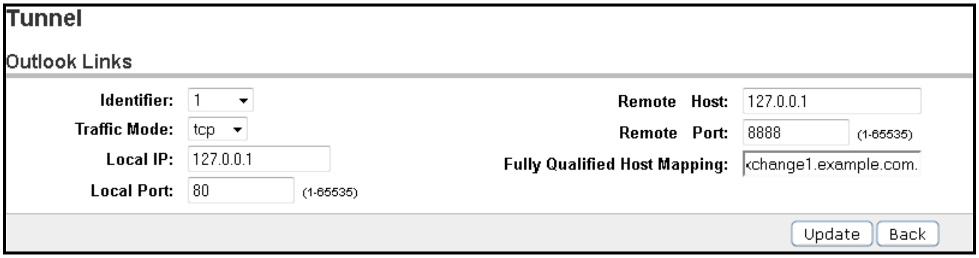
The Tunnel form is redisplayed.

28. **Click Add to create another port forwarder (if required).**

The services provided by the Exchange server (for example, mail, calendar, and address book) 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.

29. **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.



Tunnel

Outlook Links

Identifier: 1

Traffic Mode: tcp

Local IP: 127.0.0.1

Local Port: 80 (1-65535)

Remote Host: 127.0.0.1

Remote Port: 8888 (1-65535)

Fully Qualified Host Mapping: xchange1.example.com.

The host entered in the Fully Qualified Host Mapping field reads `exchange2.example2.com`.

30. **Click Update.**

31. **In portal Link form, click on General tab.**

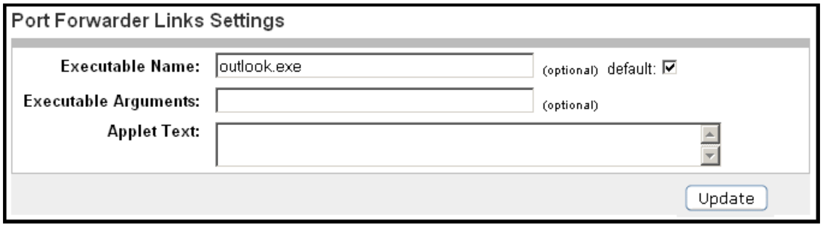
32. **Enter the application specifics.**

33. **Under Port Forwarder Links Settings, 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 would 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



Port Forwarder Links Settings

Executable Name:	outlook.exe	(optional) default: ☑
Executable Arguments:		(optional)
Applet Text:		

34. **In the Applet Text field, enter a custom text (e.g. with user instructions) to be displayed in the Java applet window (optional).**

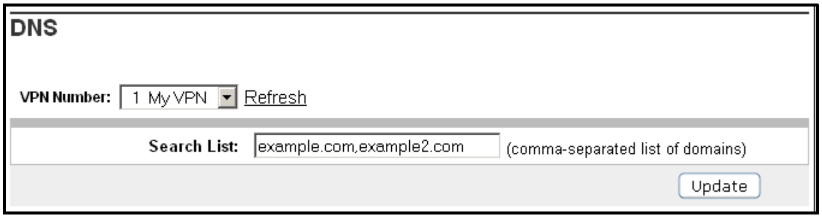
    See example 7a for a more detailed description of this step.

35. **Click Update.**

36. **In the System tree view, expand VPN Gateways and Gateway Setup and select DNS.**

37. **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 identified in Step 26 and Step 29, the following domain names must be entered.



DNS

VPN Number: 1 My VPN Refresh

Search List: example.com,example2.com (comma-separated list of domains)

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

Port Forwarder API

The Avaya VPN Gateway 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/nortel_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 (e.g. a Flash movie) which, in turn, may include embedded links to other web pages. If a user executes such an embedded link, the HTTP request may not reach the Avaya 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 Avaya 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present go to Step 10.**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

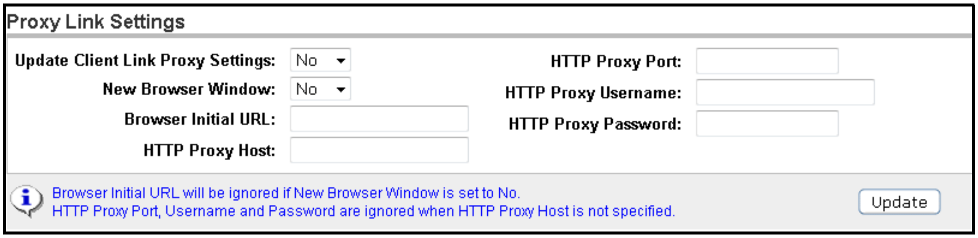
   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. Click Add.

Add Portal Links form is displayed.



Proxy Link Settings

Update Client Link Proxy Settings:	No	HTTP Proxy Port:	
New Browser Window:	No	HTTP Proxy Username:	
Browser Initial URL:		HTTP Proxy Password:	
HTTP Proxy Host:			

Browser Initial URL will be ignored if New Browser Window is set to No.
HTTP Proxy Port, Username and Password are ignored when HTTP Proxy Host is not specified.

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. Under Proxy Link Settings, 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 (e.g. 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 Browser 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 Avaya 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 Avaya VPN Gateway, 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 and 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 Avaya VPN Gateway 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 is displayed.

2. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.

3. **Under Settings, click on Link Sets.**

   Portal Linksets form is displayed.

4. **If Portal Linkset is already present go to Step 10.**

5. **Click Add.**

   Add a Portal Linkset form is displayed.

6. **In the Name field, enter the name of the current linkset.**

   The linkset name should be used later to map the linkset to a group. In this example the linkset is called `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, e.g. `<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.**

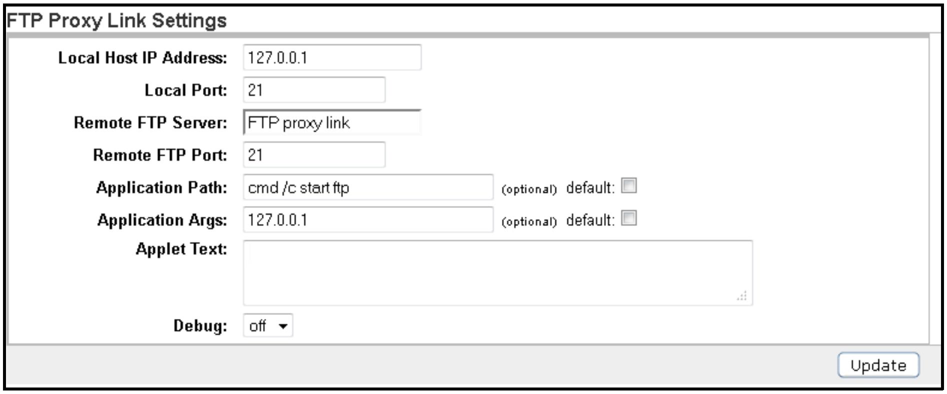
   Portal linkset ID will be added to the database.

10. **Click on the Portal Linkset name and then on Portal Links tab.**

    Portal Links form is displayed.

11. **Click Add.**

    The Add Portal Links form is displayed.



FTP Proxy Link Settings

Local Host IP Address:	127.0.0.1
Local Port:	21
Remote FTP Server:	FTP proxy link
Remote FTP Port:	21
Application Path:	cmd /c start ftp (optional) default: □
Application Args:	127.0.0.1 (optional) default: □
Applet Text:	
Debug:	off

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. **Under FTP Proxy Link Settings, 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 Avaya 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 Avaya 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, e.g. **`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 Step 15.

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 Step 15.

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 e.g. 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 Chapter 7, “Net Direct”.

Secure Portable Office

When a user logs in the SPO client, a message “Later Version of software is available” appears. If you wish to continue to load the software, select **Yes** else select **No**. This enables the SPO server to check for the latest software.

For more information on Secure Portable Office, see Chapter 13, “Secure Portable Office Client.

CHAPTER 12
HTTP to HTTPS Redirection

This chapter describes how to configure the Avaya VPN Gateway to automatically transform an HTTP client request into the required HTTPS request. By configuring such a redirect service on the Avaya VPN Gateway, the user can simply enter the fully qualified domain name in the web browser's address field, without having to specify (or knowing) the protocol required to establish a secure connection.

The redirect service is configured by adding an additional virtual HTTP server. When the virtual HTTP server on the Avaya VPN Gateway receives a request, it will redirect the browser to the virtual HTTPS server by sending an HTTP Location header to the browser.

This configuration example assumes that you have already set up a working HTTPS server for the Portal. If not, see Chapter 5, "Clientless Mode".

NOTE – During the initial setup you had the option to configure HTTP to HTTPS redirection automatically.

Configure HTTP to HTTPS Redirection

1. **Log in to the BBI as administrator.**
2. **In the System tree view, select SSL Offload Servers**

   The Servers form is displayed.
3. **Click Add.**

   The Add New Server form is displayed.

4. **In the IP address field, enter the desired virtual server IP address.**

   This is the address the client will connect to. It will typically be the same as the address of the portal HTTPS server.

5. **In the Port field, change the value to `80`.**

   Each time you create a new virtual server, the listen port is automatically set to 443. For the HTTP to HTTPS redirect service in this example, the virtual HTTP server must be set to listen to port 80 (the default port used for HTTP).

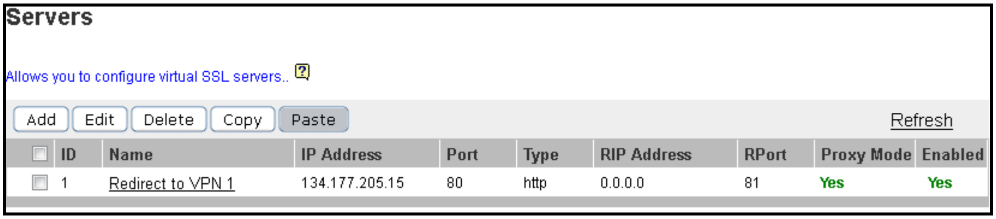
NOTE – If you have previously enabled HTTP access to the BBI through port 80, changing the port value to 80 for this server will fail. Change the BBI port to 81 (under Administration>Web) before you proceed. To access the BBI in the future you will have to append `:81` to the BBI URL, e.g. `http://10.1.82.144:81`.

---

6. **In the SSL Status list box, select `disabled`.**

7. **Click Create Server.**

   The new server is added to the servers list.



Servers

Allows you to configure virtual SSL servers..

□	ID	Name	IP Address	Port	Type	RIP Address	RPort	Proxy Mode	Enabled
□	1	Redirect to VPN 1	134.177.205.15	80	http	0.0.0.0	81	Yes	Yes

8. **Select the check box located far left on the row corresponding to the newly created server and click Edit (or click the server name).**

   The Server Settings form is displayed.

9. **In the Type list box, select `http`.**

10. **Click Update.**

11. **In the System tree view, select HTTP Type.**

    The HTTP General Settings screen is displayed.

12. **Select HTTPS Redirect.**

    The HTTPS Redirect form is displayed.

CHAPTER 13
Secure Portable Office Client

This chapter describes how to configure Secure Portable Office (SPO) client. The SPO client provides remote access for client corporate networks and other third party applications.

NOTE – The SPO menu is enabled only after SPO license is installed. Also this menu is not visible when the VPN type is contivity. For more information about licenses see, “Licenses” on page 73.

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

- Avaya Basic– contains basic software with i2050 and One-X soft client.
- Avaya Contact Center (ACC)– contains all the applications and software of Avaya Basic with the addition of Avaya Contact Center Express Desktop 5.0.

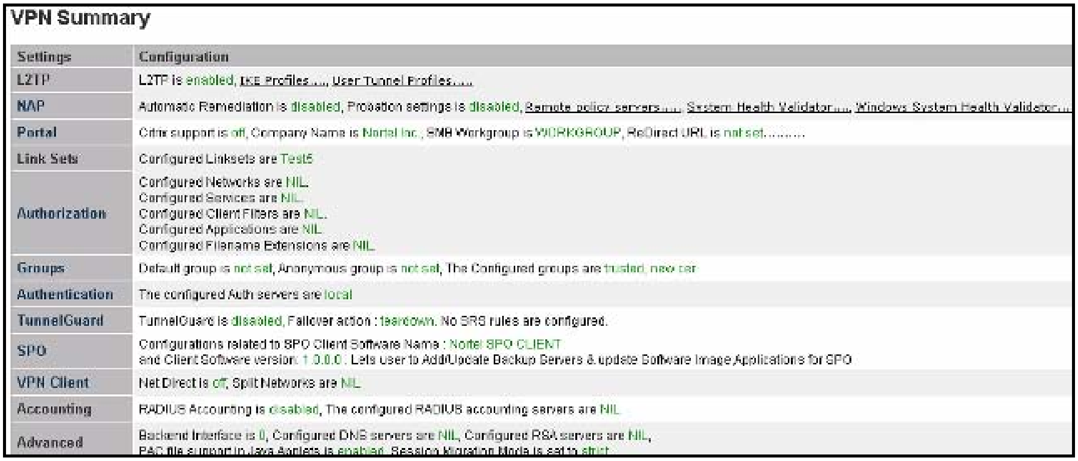
For more information about Installation and Configuration of SPO client, see *Configuration - Secure Portable Office Client* (NN46120-301).

Configure SPO General Settings

Use the General Settings form to change the settings for the SPO. The following procedure describes how to configure general settings.

1. **Login as system administrator.**
2. **Click on Config tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Click on the VPN Gateway name.**

   The following VPN summary screen appears.



VPN Summary

Settings	Configuration
L2TP	L2TP is enabled, IKE Profiles . . . ., User Tunnel Profiles. . . .
NAP	Automatic Remediation is disabled, Probation settings is disabled, Remote policy servers. . . ., System Health Validator. . . ., Windows System Health Validator. . .
Portal	Citrix support is off, Company Name is Nortel Inc. , SMB Workgroup is WORKGROUP, ReDirect URL is not set. . . . .
Link Sets	Configured Linksets are Test5
Authorization	Configured Networks are NIL. Configured Services are NIL. Configured Client Filters are NIL. Configured Applications are NIL. Configured Filename Extensions are NIL.
Groups	Default group is not set, Anonymous group is not set, The Configured groups are trusted, new cer
Authentication	The configured Auth servers are local
TunnelGuard	TunnelGuard is disabled, Failover action : teardown. No SRS rules are configured.
SPO	Configurations related to SPO Client Software Name : Nortel SPO CLIENT and Client Software version: 1.0.0.0 . Lets user to Add/Update Backup Servers & update Software Image,Applications for SPO
VPN Client	Net Direct is off, Split Networks are NIL.
Accounting	RADIUS Accounting is disabled, The configured RADIUS accounting servers are NIL.
Advanced	Backend Interface is 0, Configured DNS servers are NIL, Configured RSA servers are NIL, PAC file support in Java Applets is enabled, Session Migration Mode is set to strict

5. **Under Settings, select SPO.**

   By default General tab is selected.

6. **Specify the SPO Client software name.**

   This is a mandatory field that contains up to 30 alphanumeric characters. This is an alphanumeric field.

7. **Specify the SPO Client minimum version.**

   This is a mandatory field.

NOTE – Version needs to match the additional software name.

---

8. **Enter the Banner/License Agreement or Warning text for SPO users.**

   If banner text is not entered by the system administrator, a blank banner page is displayed.

9. **Specify the SPO client logo file.**

10. **Specify the system icon file for the SPO Client.**

NOTE – SPO Logo and System Icon can be imported using protocol scheme for example, ftp, tftp, scp, and sftp. The size of SPO Logo and System Icon should not be more than 1MB.

---

11. **Click Update, and click Apply to apply the changes.**

NOTE – Click Logo Restore and Sys Icon Restore buttons to restore the default settings for the logo and system tray icon, respectively. The default logo and default system tray icon are part of the VPN Gateway.

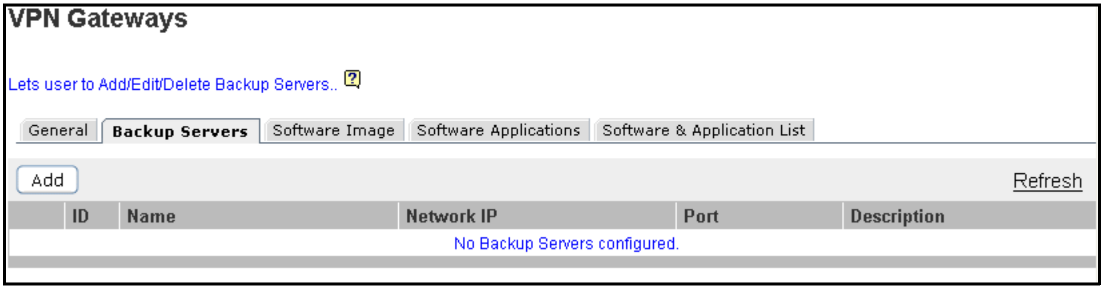
Adding a Backup Server

When the SPO client connects successfully to the server, SPO retrieves list of all the servers. For subsequent SPO client connections, if a failure in occurs the primary server, the SPO client can use the backup server to connect. The following procedure explains how to add a backup server.

1. **Login as system administrator.**
2. **Click on Config tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Click on the VPN Gateway name.**

   VPN Summary screen is displayed.
5. **Under Settings, select SPO.**
6. **Click on the Backup Server tab.**

   Backup Servers window appears.



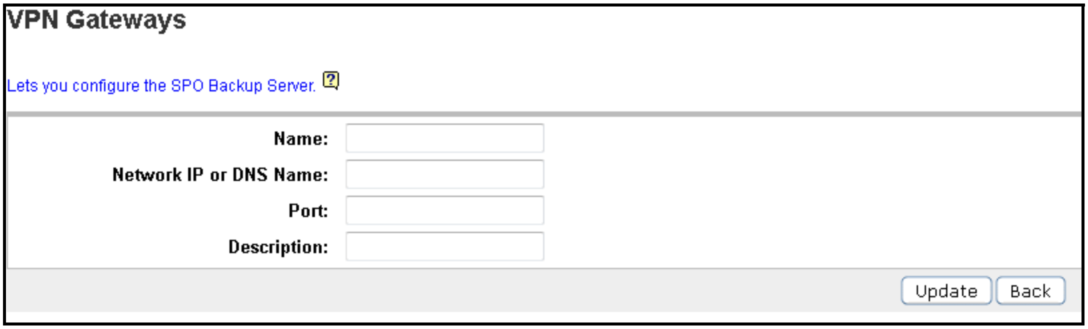
VPN Gateways

Lets user to Add/Edit/Delete Backup Servers..

	ID	Name	Network IP	Port	Description
			No Backup Servers configured.		

7. **Click Add.**

Backup Servers Add/Update window appears.



VPN Gateways

Lets you configure the SPO Backup Server.

Name:

Network IP or DNS Name:

Port:

Description:

8. **Specify a name for the backup server. This is a mandatory field.**

9. **Specify the Network IP or DNS name for the current backup server. This is a mandatory field.**

10. **Specify the port for the current backup server. This is a mandatory field.**
    The Port must be a positive integer less than or equal to 65535.

11. **Specify the description for the current backup server.**

12. **Click Update, and click Apply to apply the changes.**

Configuring Software Image

You can upload SPO client software images in the VPN Gateway. Users with access rights can access these images through the VPN portal and login to the SPO client. The following procedure explains how to configure the software images.

1. **Login as system administrator.**

2. **Click on Config tab.**

3. **In the system tree view, select VPN Gateways.**

4. **Click on the VPN Gateway name.**

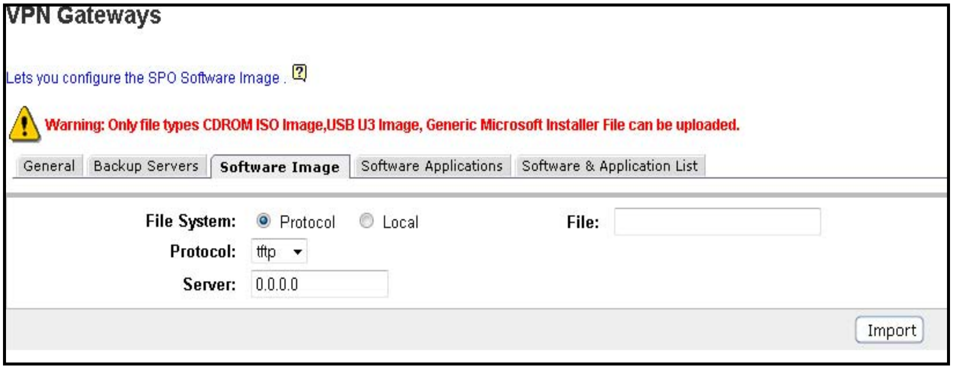
   VPN Summary screen is displayed.

5. **Under Settings, select SPO.**

6. **Click on the Software Image tab.**

   Software Image screen appears.

7. **Select the file system: local or protocol to configure the SPO.**



VPN Gateways

Lets you configure the SPO Software Image .

Warning: Only file types CDROM ISO Image,USB U3 Image, Generic Microsoft Installer File can be uploaded.

File System: ● Protocol ○ Local

File:

Protocol: tftp

Server: 0.0.0.0

NOTE – Select protocol if you want to transfer the file using a file system protocol. If you want to transfer file locally go to Step 14.

---

8. **Select the protocol type: ftp, tftp, scp, or sftp.**
9. **Specify the IP address or host name of the server from which file needs to be imported.**
10. **Specify the file name on the server.**
11. **Specify the user name to import the file.**
12. **Specify the password for the user to import the file.**

NOTE – The User and Password fields are prompted only for the protocols: ftp, scp,or sftp.

---

13. **Click Import to import the file.**
14. **Select Local if you want to transfer the file locally.**
15. **Specify the name of the file which you want to upload to the VPN Gateway.**
16. **Click Import, to import the file in the VPN Gateway.**

NOTE – You can upload only file types CDROM ISO Image, U3 USB Image (U3P), Generic Microsoft Installer File (MSI).

Adding application software

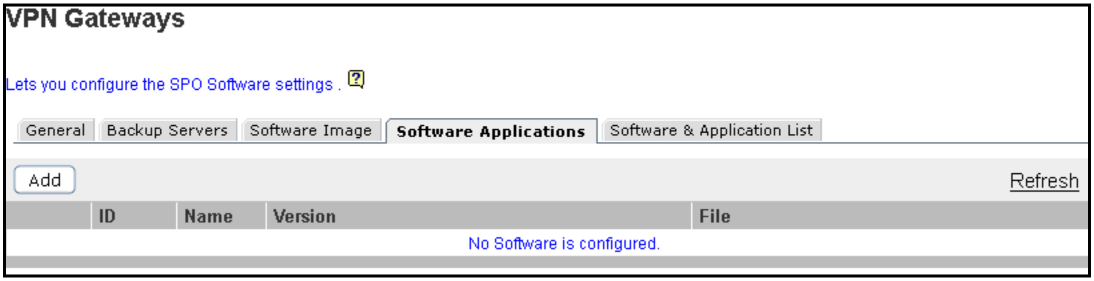
Users can add the following software in the VPN Gateway:

- **Third party software**- You can upload only zip files in the VPN Gateway.
- **Software upgraded for SPO client** - You can upload U3 package, MSI files in the VPN Gateway.

This procedure explains how to add a SPO Client software. This software is used to exchange the credentials between the AVG server and the SPO Client software.

1. **Login as system administrator.**
2. **Click on Config tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Click on the VPN Gateway name.**

   VPN Summary screen appears.
5. **Under Settings, select SPO.**
6. **Click on the Software tab.**

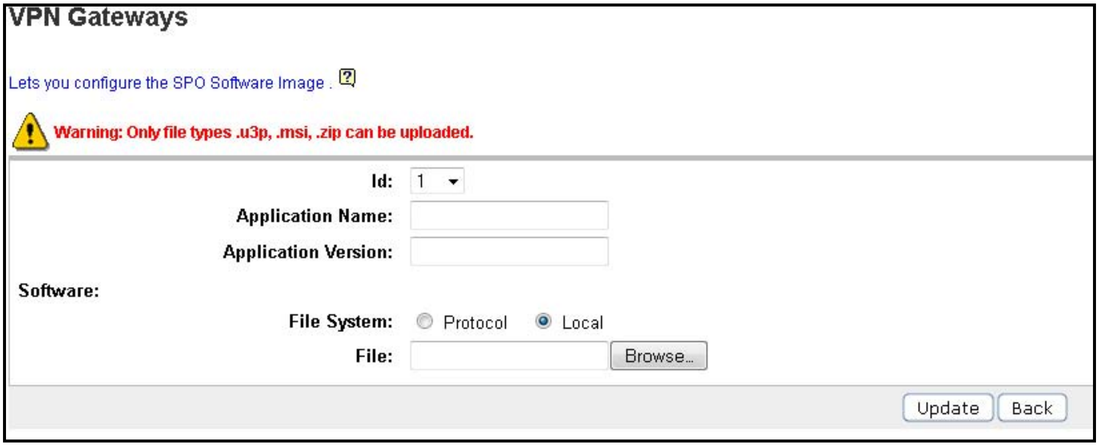


VPN Gateways

Lets you configure the SPO Software settings .

	ID	Name	Version	File
No Software is configured.				

7. **Click Add to add the software.**



VPN Gateways

Lets you configure the SPO Software Image .

Warning: Only file types .u3p, .msi, .zip can be uploaded.

Id:	1
Application Name:	
Application Version:	
Software:	
File System:	○ Protocol ● Local
File:	

8. **Select an ID for the current software.**

9. **Specify the name of the current software.**

   The software name should not be more than 15 characters except “”.

10. **Specify the version for the current software.**

    The software version must be only numeric and match the actual software version (except for any letters used in the actual software version).

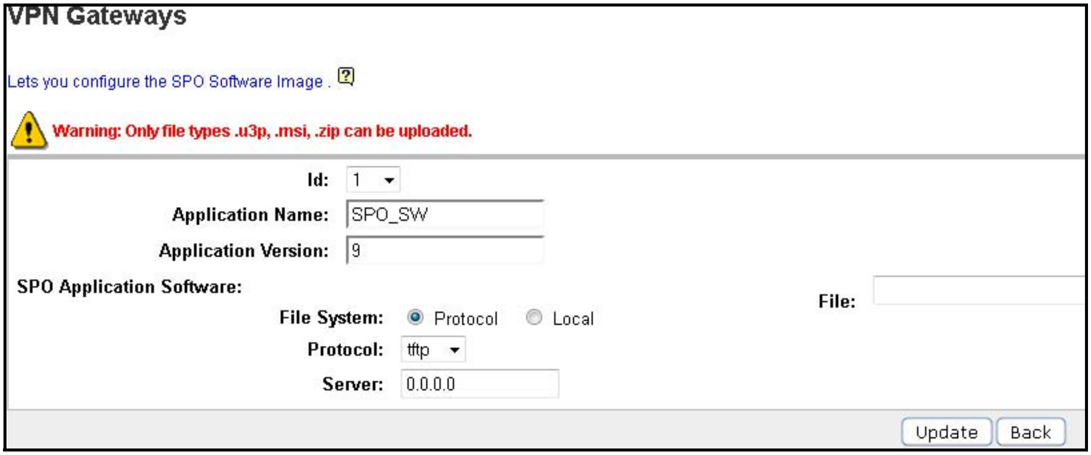
11. **Select the following file system to add a new software to the SPO:**

    local - files are located on PC

    protocol - file transfer protocol --- files are on server

NOTE – You can place the newer versions of the SPO Client software (u3p and msi) in the file system to allow automated notification to the user that a more recent version of software is available for download.

12. **Select protocol if you want to transfer the file using a file system Protocol. If you want to transfer the software locally, go to Step 18.**



VPN Gateways

Lets you configure the SPO Software Image .

Warning: Only file types .u3p, .msi, .zip can be uploaded.

Id: 1

Application Name: SPO_SW

Application Version: 9

SPO Application Software:

File System: ● Protocol ○ Local

Protocol: tftp

Server: 0.0.0.0

File:

13. **Import the files using one of the system protocols: ftp, tftp, scp, or sftp.**

14. **Specify the file name on the server.**

15. **Specify the user name to import the file.**

16. **Specify the password for the user to import the file.**

> **NOTE –** The User and Password fields are prompted only for the protocols: ftp, scp,or sftp.

17. **Click Update.**

18. **Select file system Local.**

19. **Specify the name of the software file that you want to upload to the VPN Gateway.**

20. **Go to Groups and enable SPO.**

    For information on these configuration steps see “Adding a Secure Portable Office software index” on page 236.

21. **Click Update.**

> **NOTE –** You need to configure the SPO Software Index under Groups to specify the applications that are accessed by the users in that group. For information on these configuration steps, see Chapter 8, “Adding a Secure Portable Office software index.

Viewing images/applications

Follow these steps to view the imported images:

1. **Login as system administrator.**
2. **Click on Config tab.**
3. **In the system tree view, select VPN Gateways.**
4. **Click on the VPN Gateway name.**

   VPN Summary screen appears.
5. **Under Settings, select SPO.**
6. **Click on the Software & Application list tab.**

   You can view the list of imported images.

CHAPTER 14
Bandwidth Management

This chapter provides procedures to configure Bandwidth Management (BWM) for the Avaya VPN Gateway device.

Bandwidth Management (BWM) enables administrators to allocate a portion of the available bandwidth for specific users or groups. The bandwidth policies take lower and upper bound. The lower bound (soft limit) is guaranteed and the upper bound (hard limit) is available according to the requirement.

The BWM provides bandwidth policy management for the user traffic and IPsec Passthrough.

The user traffic is classified based on the group the user is placed. Based on the user source IP address, a filter is added to mark the traffic coming from the user to a particular queue. After adding the source IP address, the incoming packets are marked based on the traffic control filter and then queued according to the configuration. You can configure bandwidth management policy for user groups and extended groups.

The BWM Internet Protocol Security (IPsec) PassThrough handles the IPSec Branch Office (BO) tunnel traffic on a different bandwidth policy and bandwidth rate. The IPSec BO tunnel traffic is classified in a separate queue and subsequently handled with a different priority based on the specified configuration.

If you use BWM on a cluster, it is possible that a user connected to one of the hosts in the cluster gets bandwidth while another user connected to another host in the cluster do not get the bandwidth. This is because the bandwidth policies are based on group and per host based; policies are not based on cluster or VPN.

For more information about configuring BWM and IPSec PassThrough servers, see:

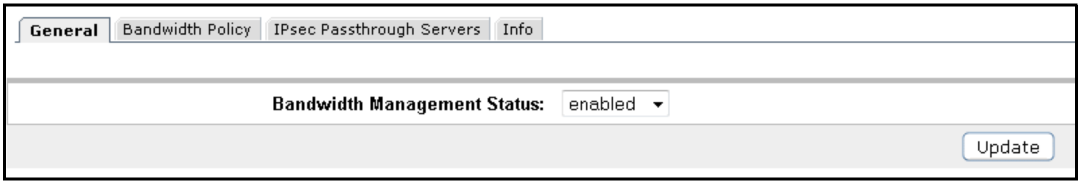
- "Enabling BWM" on page 442
- "Configuring BWM policy" on page 442
- "Configuring IPsec PassThrough Servers" on page 443
- "Setting BWM information type" on page 444

Enabling BWM

To enable BWM, perform the following:

1. **Log on to the BBI as an administrator user.**
2. **From the System tree view, select Bandwidth Management.**

   The Bandwidth Management form appears.



Bandwidth Management Status: enabled

3. **Click the General tab.**
4. **From the Bandwidth Management Status list, select enabled.**
5. **Click Update.**

Configuring BWM policy

To configure BWM policy, perform the following steps:

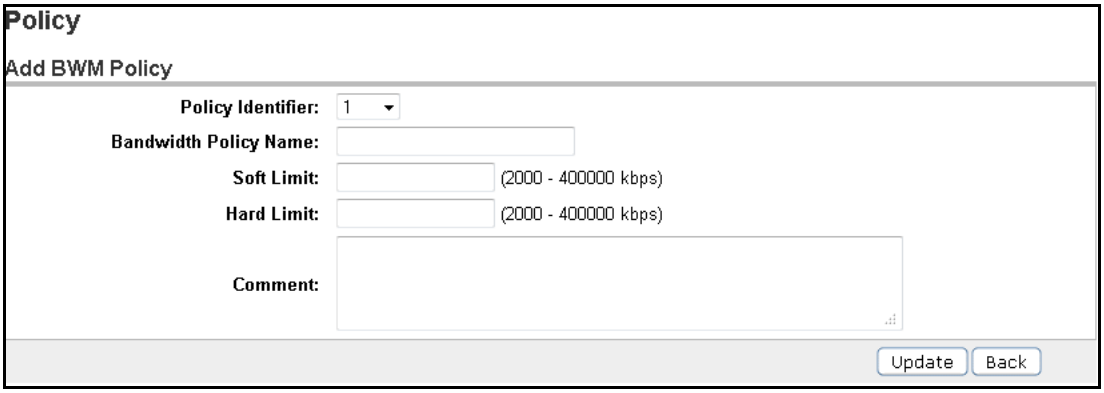
1. **Log on to the BBI as an administrator user.**
2. **From the System tree view, select Bandwidth Management**

   The Bandwidth Management Policy form appears.
3. **Select the Bandwidth Policy tab.**

   The Bandwidth Policy form appears.

4. **Click Add.**

   The Add BWM Policy form appears.



Policy

Add BWM Policy

Policy Identifier:	1
Bandwidth Policy Name:	
Soft Limit:	(2000 - 400000 kbps)
Hard Limit:	(2000 - 400000 kbps)
Comment:	

5. **From the Policy Identifier list, select an index for the BWM policy.**

6. **In the Bandwidth Policy Name field, enter the BWM policy name.**

7. **In the Soft Limit field, enter the soft limit for the policy.**

   The soft limit can be from 2000 to 400000.

8. **In the Hard Limit field, enter the hard limit for the policy.**

   The hard limit can be from 2000 to 400000.

9. **In the Comment field, enter the comment for reference.**

10. **Click Update.**

    The BWM policy is added to the list.

Configuring IPsec PassThrough Servers

To configure IPsec Passthrough Servers, perform the following:

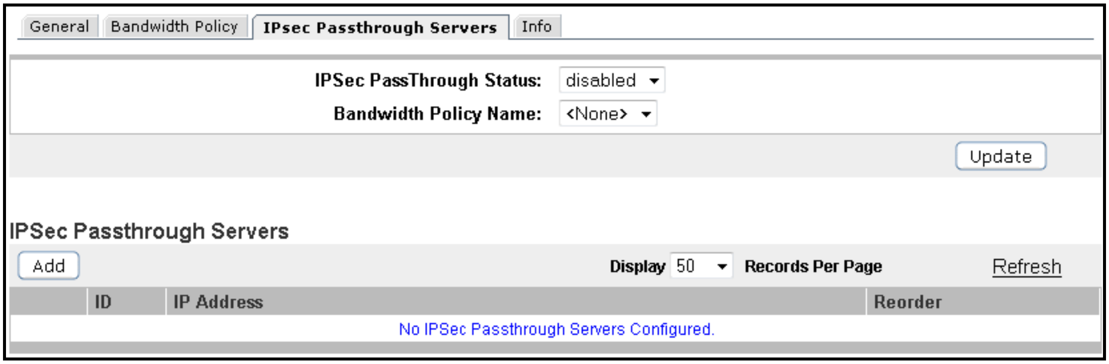
1. **Log on to the BBI as an administrator user.**

2. **From the System tree view, select Bandwidth Management.**

   The Bandwidth Management form appears.

3. **Select IPsec Passthrough Servers.**

   The IPsec Passthrough Servers form appears.



IPSec PassThrough Status: disabled

Bandwidth Policy Name: <None>

IPSec Passthrough Servers

Display 50 Records Per Page

ID	IP Address	Reorder
	No IPSec Passthrough Servers Configured.	

4. **From the IPsec PassThrough Status list, select enabled.**
5. **From the Bandwidth Policy Name list, select BWM policy name.**
6. **Click Update.**
7. **Click Add.**

   The Add New IPSec Passthrough Server form appears.

8. **In the IP Address field, enter the IP address for the IPsec PassThrough Server.**
9. **Click Update.**

   The IPsec Passthrough Server is added to the list.

Setting BWM information type

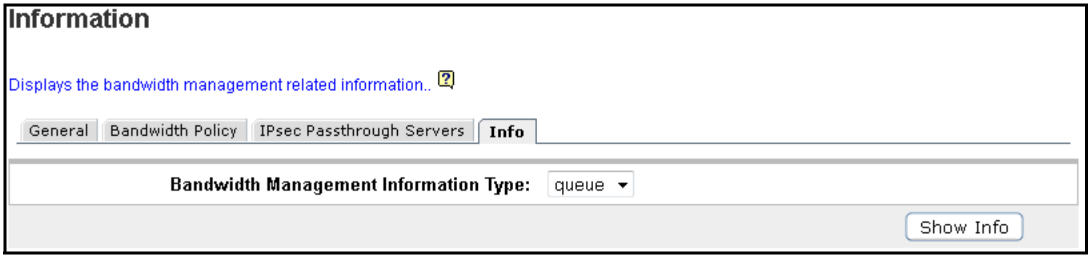
To set Bandwidth Management information type, perform the following:

1. **Log on to the BBI as an administrator user.**
2. **From the System tree view, select Bandwidth Management.**

   The Bandwidth Management form appears.

3. **Select the Info.**

   The Info form appears.



Information

Displays the bandwidth management related information..

Bandwidth Management Information Type: queue

4. **From the Bandwidth Management Information Type list, select one of the following:**

   queue, to view the queues created.

   Or

   class, to view the class.

   Or

   filter, to view the filters.

5. **Click Show Info.**

   The bandwidth information for the selected information type appears.

CHAPTER 15

Configure Avaya Endpoint Access Control Agent

This chapter describes how to configure the Avaya VPN Gateway for use with Avaya Endpoint Access Control Agent (EACA). Avaya Endpoint Access Control Agent is an application that checks that the required components (for example, executables, DLLs, and configuration files) are installed and active on the remote user's machine.

How is Avaya Endpoint Access Control Agent Activated?

For HTTPS connections, the Avaya Endpoint Access Control Agent *applet* is downloaded to the client machine and started as soon as the user has successfully logged in to the Portal.

For Avaya VPN Client connections, the Avaya Endpoint Access Control Agent *agent* (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 #>EACA>SRS Rules**.

When Avaya Endpoint Access Control Agent is finished 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 behavior is configurable. Either the session/tunnel can be torn down or the user may be granted restricted access.

If needed, a specific Avaya Endpoint Access Control Agent SRS rule administrator can be created. The SRS rule administrator is only granted access to the Avaya Endpoint Access Control Agent Admin applet. For instructions on how to create an administrator user in the CLI, see "Managing User and Groups" in the *User's Guide*.

Configure SRS Rules

Avaya Endpoint Access Control Agent SRS rules can only be configured in the BBI (not in the CLI).

Log in to the BBI and Launch the Avaya Endpoint Access Control Agent Applet

1. **Logon to the BBI as administrator.**

2. **Click Config tab.**

3. **Select VPN Gateways.**

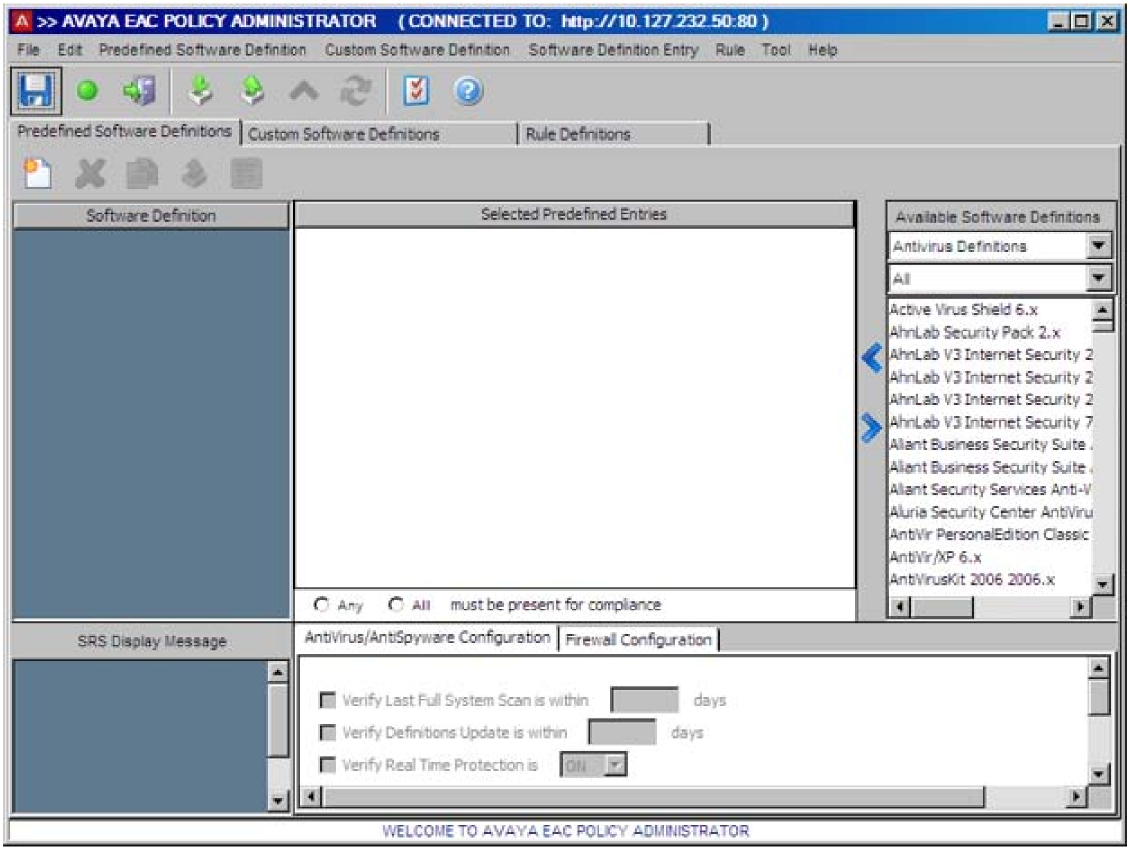
4. **Select the VPN Gateway name.**

5. **Under Settings, select EACA.**

6. **Select the SRS Rules tab.**

7. **Click Launch.**

The EACA applet used for configuring SRS rules is displayed.


>> AVAYA EAC POLICY ADMINISTRATOR   (CONNECTED TO: http://10.127.232.50:80)
File   Edit   Predefined Software Definition   Custom Software Definition   Software Definition Entry   Rule   Tool   Help
Predefined Software Definitions
Custom Software Definitions
Rule Definitions
Software Definition
Selected Predefined Entries
Available Software Definitions
Antivirus Definitions
All
Active Virus Shield 6.x
AhnLab Security Pack 2.x
AhnLab V3 Internet Security 2
AhnLab V3 Internet Security 2
AhnLab V3 Internet Security 2
AhnLab V3 Internet Security 7
Aliant Business Security Suite
Aliant Business Security Suite
Aliant Security Services Anti-V
Aluria Security Center AntiViru
AntiVir PersonalEdition Classic
AntiVir/XP 6.x
AntiVirusKit 2006 2006.x
○ Any   ○ All   must be present for compliance
SRS Display Message
AntiVirus/AntiSpyware Configuration
Firewall Configuration
□ Verify Last Full System Scan is within days
□ Verify Definitions Update is within days
□ Verify Real Time Protection is ON
WELCOME TO AVAYA EAC POLICY ADMINISTRATOR

Avaya Endpoint Access Control Agent Options

Following are the list of buttons and their functions used in the Avaya Endpoint Access Control Agent Applet:

Table 1

Button	Function
🗋	Creates new rule, entry, or definition.
✖	Deletes new rule, entry, or definition.
⧉	Copies new rule, entry, or definition.
⬆	Exports new rule, entry, or definition.
⬇	Imports new rule, entry, or definition.
🗎	Displays message contents of Predefined and Custom software definition entries.

🟢	Sets the Contivity for Avaya Endpoint Access Control Agent.
➡	Exits from Avaya Endpoint Access Control Agent.
⌃	Displays memory snapshot.
↘	Refreshes memory snapshot.
☑	Sets the preferences for the Avaya Endpoint Access Control Agent.
📁	Creates new disk entry.
🗔	Creates new memory module entry.
⧉	Creates new registry entry.

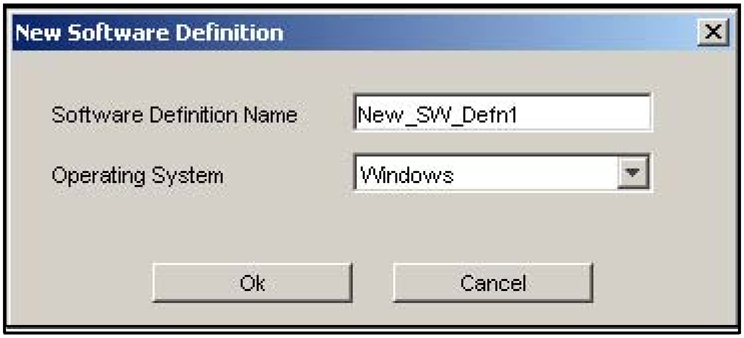
Create New Predefined Software Definitions

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.



New Software Definition

Software Definition Name: New_SW_Defn1

Operating System: Windows

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 Avaya Endpoint Access Control Agent rule validation:**
    - Any - Any of the predefined entries are validated.
    - All - Any of the predefined entries are validated.
5. **Specify the AntiVirus\Antispyware Configuration and Firewall Configuration parameters for 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:

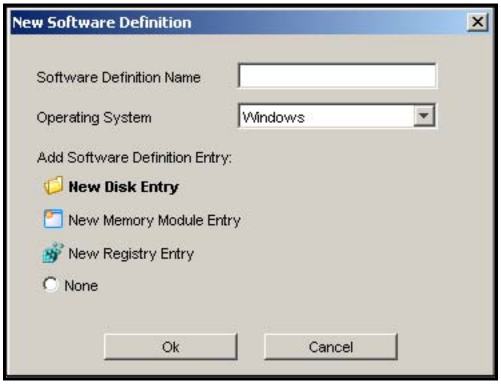
- Select multiple Software Definitions by clicking export to export selected entries.
- Select multiple rules.
- Export all Rules and definitions by a single click
- Import older versions of definitions.

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.



New Software Definition

Software Definition Name

Operating System: Windows

Add Software Definition Entry:

- **New Disk Entry**
- New Memory Module Entry
- New Registry Entry
- ○ None

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. For more information, see the section "Set Avaya Endpoint Access Control Agent Preferences" on page 465.

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 Avaya Endpoint Access Control Agent to verify that certain files are *not* present on the client system.

1. **Click on the Custom Software Definitions tab.**

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.**

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 anew 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. **Click OK.**

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 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.

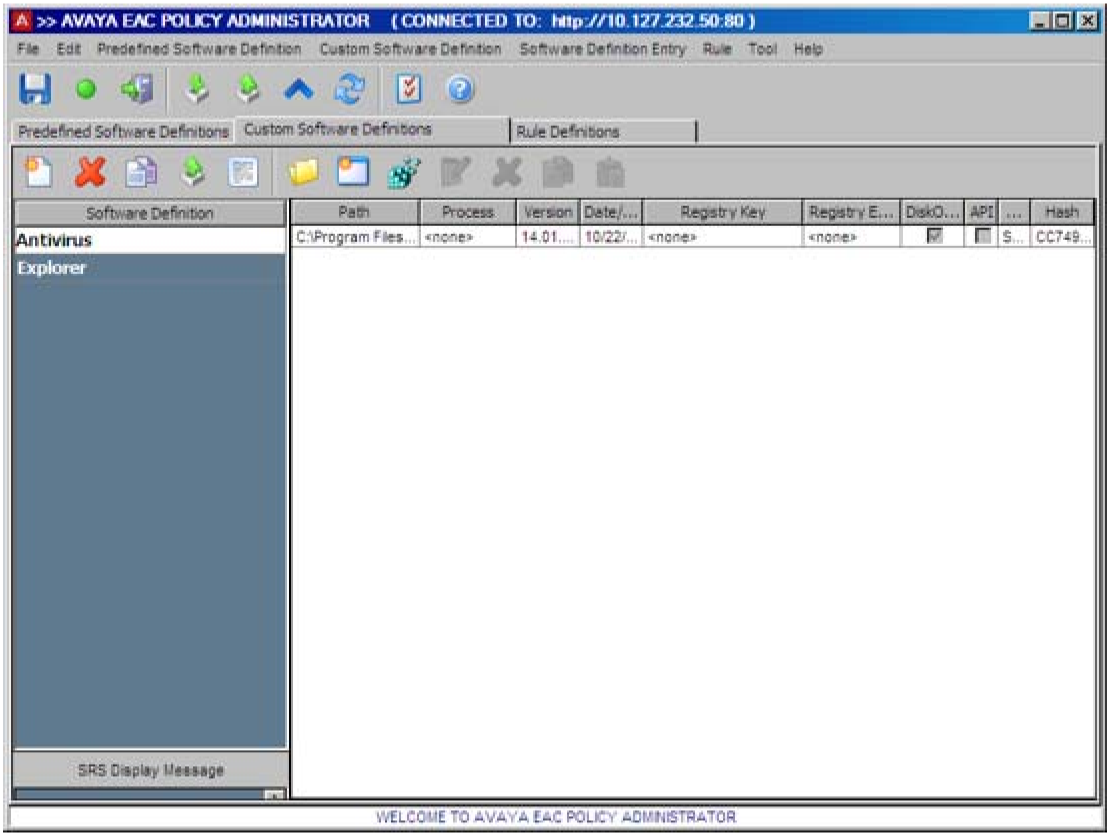
Having created a logical expression with the desired conditions, simply select the expression for the Avaya Endpoint Access Control Agent SRS rule.

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 an so on.

2. **Click on Rule Definitions tab.**

Avaya Endpoint Access Control Agent rules and expressions with the same names as the software definitions have been created and appear on the Rule Definitions tab.



>> AVAYA EAC POLICY ADMINISTRATOR (CONNECTED TO: http://10.127.232.50:80)
File
Edit
Predefined Software Definition
Custom Software Definition
Software Definition Entry
Rule
Tool
Help
Predefined Software Definitions
Custom Software Definitions
Rule Definitions
Software Definition
Antivirus
Explorer
SRS Display Message
WELCOME TO AVAYA EAC POLICY ADMINISTRATOR

Path	Process	Version	Date/...	Registry Key	Registry E...	DiskO...	API	...	Hash
C:\Program Files...	<none>	14.01....	10/22/...	<none>	<none>	☑	□	S...	CC749...

In the preceding example, two Avaya Endpoint Access Control Agent rules have been created, each defining a unique application. To create *one* Avaya Endpoint Access Control Agent 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.

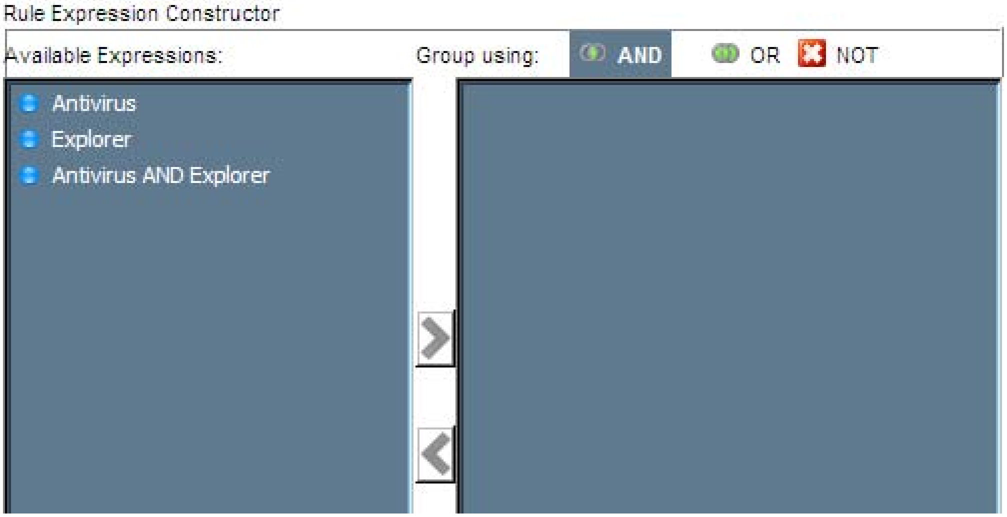
4. **Select another expression that you will use to form a new logical expression in combination with the first.**

5. **Using the radio buttons, select the type of expression you wish to construct, in this example an AND expression.**

The AND operand lets you construct a logical expression where *both* conditions must be met for the Avaya Endpoint Access Control Agent checks to pass. The OR operand lets you construct an expression where *either* of the conditions must be met for the Avaya Endpoint Access Control Agent checks to pass. The NOT operand lets you construct an expression where the condition *must not* be met for the Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent Rule Expression.**

   A new expression is created and copied to the Available Expressions area.



7. **To create a Avaya Endpoint Access Control Agent rule, click on Rules Definitions tab. You can create a rule by using the following methods:**

   - From Avaya Endpoint Access Control Agent Rule menu, select New Avaya Endpoint Access Control Agent Rule.
   - Click on New Avaya Endpoint Access Control Agent Rule button.

   The New Avaya Endpoint Access Control Agent Rule window appears.

8. **Enter a name for the Avaya Endpoint Access Control Agent rule and click OK.**

   The new rule name appears in the Avaya Endpoint Access Control Agent Rule Name column.

9. **In the Avaya Endpoint Access Control Agent 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

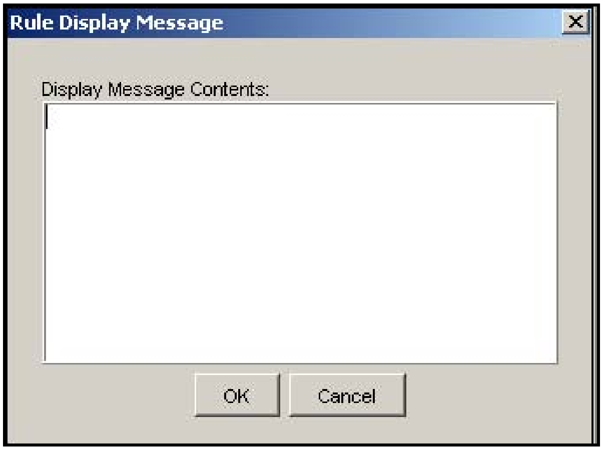
By adding a Avaya Endpoint Access Control Agent rule message to a Avaya Endpoint Access Control Agent rule, you can provide important information to the user, for example the reason why the Avaya Endpoint Access Control Agent checks failed and/or the recommended action. This information is expanded by the `<var:tgFailureReason>` variable, along with the Avaya Endpoint Access Control Agent 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 page 487).

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.**



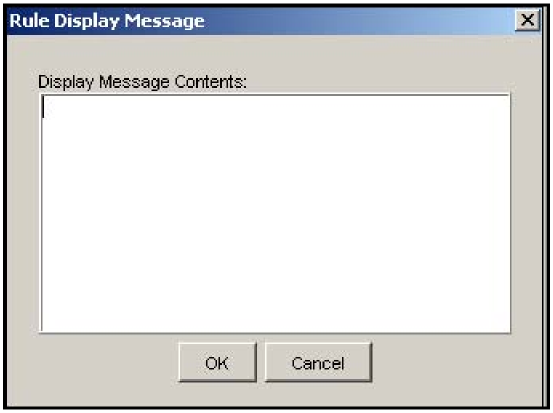
4. **Type the message and click OK.**

   The message is displayed at the left side of the screen.

Add Predefined Software Definition Message

The software definition comment is shown in the message displayed when the user clicks the **details** link on the Portal login page (see page 487). It is also included in the `<var:eacFailureDetail>` variable. The variable can for example be included in a linkset text to print the result of a Avaya Endpoint Access Control Agent 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.**

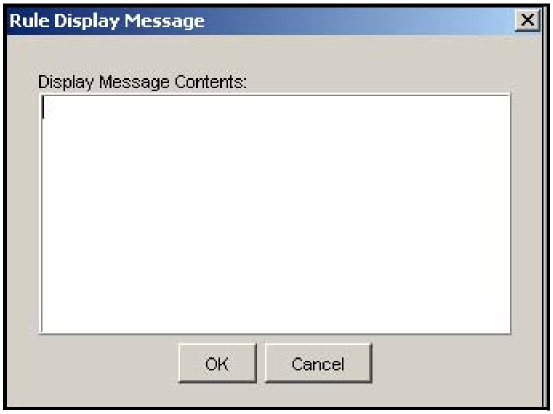


3. **Type in the desired text and click OK.**

Add Custom Software Definition Message

Follow these steps to add a message to custom software definition:

1. **Click on Custom Software Definitions tab.**
2. **Select Predefined Software Definition menu.**



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.**

Delete a Custom Software Definition

Follow these steps to delete a custom software definition:

1. **Click on Custom Software Definitions tab.**
2. **In the Software Definition column, select the desired software definition.**
3. **On the Custom Software Definition menu, select Delete Definition.**

Delete a Avaya Endpoint Access Control Agent Rule

Follow these steps to delete a Avaya Endpoint Access Control Agent rule:

1. **Click on the Rule Definitions tab.**
2. **In the Rule table, select the desired rule.**
3. **Under menu, select the Avaya Endpoint Access Control Agent Rule option.**
4. **Click on Delete Avaya Endpoint Access Control Agent Rule option under it.**
5. **Click Yes.**

Delete an Expression

1. **Click the Rule Definitions tab.**
2. **In the Available Expressions area, select the desired expression and click the Delete Expression button.**

NOTE – Note that you cannot delete an expression that is used in a Avaya Endpoint Access Control Agent 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 is displayed.

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 Rum 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.

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.

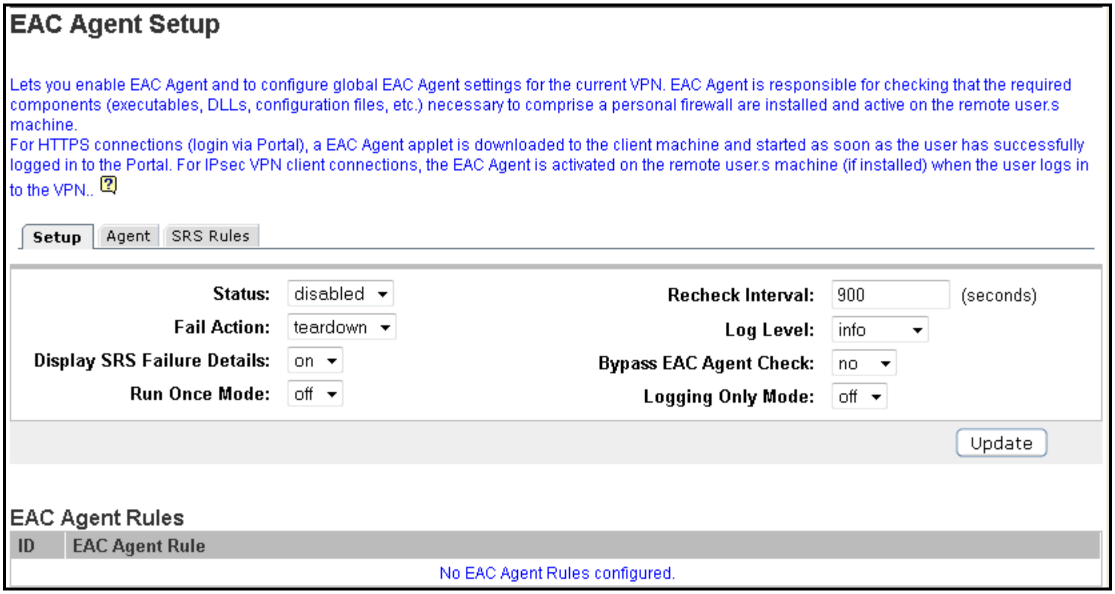
Configure Avaya Endpoint Access Control Agent

This section includes an example of how to set up a working Avaya Endpoint Access Control Agent solution. It illustrates how to configure Avaya Endpoint Access Control Agent to check that the proper anti-virus program is installed on the remote user’s machine and – if the Avaya Endpoint Access Control Agent 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. **Logon to the BBI as administrator.**
2. **Click Config tab.**
3. **Select VPN Gateways.**
4. **Select the VPN Gateway name.**
5. **Select EACA.**
6. **Select the Setup tab.**

The EACA Setup form is displayed.



EAC Agent Setup

Lets you enable EAC Agent and to configure global EAC Agent settings for the current VPN. EAC Agent is responsible for checking that the required components (executables, DLLs, configuration files, etc.) necessary to comprise a personal firewall are installed and active on the remote user.s machine.

For HTTPS connections (login via Portal), a EAC Agent applet is downloaded to the client machine and started as soon as the user has successfully logged in to the Portal. For IPsec VPN client connections, the EAC Agent is activated on the remote user.s machine (if installed) when the user logs in to the VPN..

Status:	disabled	Recheck Interval:	900 (seconds)
Fail Action:	teardown	Log Level:	info
Display SRS Failure Details:	on	Bypass EAC Agent Check:	no
Run Once Mode:	off	Logging Only Mode:	off

EAC Agent Rules

ID	EAC Agent Rule
	No EAC Agent Rules configured.

7. **In the Status list box, select enabled.**

8. **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 Avaya Endpoint Access Control Agent checks fail. By setting the action to restricted, the remote user can be given limited access if the Avaya Endpoint Access Control Agent checks fail. In this example we will set the fail action to restricted.

9. **In the Run Once Mode, select on.**

   When this option is enabled, the client runs SRS checks only one time and the resulting access is provided until the session logout. The run once mode is applicable only for the portal and SPO clients. It also prevents session exit due to heartbeat timeout and rechecks.

10. **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 Avaya Endpoint Access Control 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

11. **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 Avaya Endpoint Access Control Agent SRS rules.

12. **In the Display SRS Failure Details list box, select the desired option.**

    This step lets you specify whether or not Avaya Endpoint Access Control Agent SRS rule failure details should be displayed to the user.

    - on: The details link is displayed on the Portal login page if the Avaya Endpoint Access Control Agent checks fail and Fail Action (see above) 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:eacFailureDetail> variable.
    - off: The details link is not displayed. The <var:eacFailureDetail> variable is not expanded.

    NOTE – This setting has no impact on the behavior of the installed Avaya Endpoint Access Control Agent agent, that is, even if the setting is disabled on the AVG, it might be enabled in the Avaya Endpoint Access Control Agent agent settings.

13. **In Bypass Avaya Endpoint Access Control Agent Check, select any one of the following option:**

    - on: Bypasses the Avaya Endpoint Access Control Agent checks for client machines with unsupported operating systems (for applet) and client machines without Avaya Endpoint Access Control Agent installed agent.
    - off: Does not bypasses the Avaya Endpoint Access Control Agent checks.

14. **In the Logging Only Mode, select any one of the following options:**

    - `on`: Lets the network administrator determine the number of compliant and noncompliant users on network without disturbing the access permissions due to SRS checks. Users are always given access based on SRS check pass.
    - `off`: Disables the logging only mode.

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

Avaya Endpoint Access Control Agent Agent Settings

The Avaya Endpoint Access Control Agent *agent* is started (if enabled) when the remote user connects to the VPN with the Avaya VPN Client in IPSec mode. Following are instructions on how to configure the Avaya VPN Gateway for use with the Avaya Endpoint Access Control Agent agent.

1. **Logon to the BBI as administrator.**
2. **Click Config tab.**
3. **Select VPN Gateways.**
4. **Select the VPN Gateway name.**
5. **Select EACA.**
6. **Select Agent.**

   The Avaya Endpoint Access Control Agent Agent form is displayed.

7. **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 Avaya Endpoint Access Control Agent server (on the Avaya VPN Gateway) to the Avaya Endpoint Access Control Agent client (on the client machine). This setting only applies to clients with the Avaya Endpoint Access Control Agent *agent* installed – not the Avaya Endpoint Access Control Agent *applet* downloaded from the Portal.

8. **In the Agent Minimum Version field, specify the minimum version of the Avaya Endpoint Access Control Agent application (agent).**

   This step lets you enter the minimum version of the Avaya Endpoint Access Control Agent agent. A VPN client with an older version of the Avaya Endpoint Access Control Agent agent will not be able to connect to the Avaya VPN Gateway. This setting only applies to clients with the Avaya Endpoint Access Control Agent *agent* installed – not the Avaya Endpoint Access Control Agent *applet* downloaded from the Portal. The default value is `0.0.0.0`, that is, all client versions are allowed.

9. **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 Avaya Endpoint Access Control Agent checks when they succeed.

1. **Logon to the BBI as administrator.**
2. **Click Config tab.**

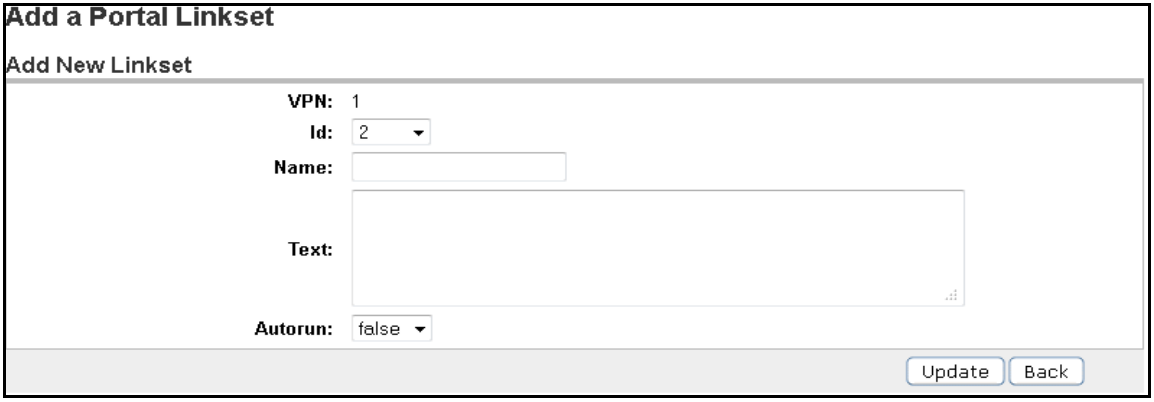
3. **Select VPN Gateways.**

4. **Select the VPN Gateway name.**

5. **Select Linkset.**

6. **Click Add.**

   The Add New Linkset form is displayed.



Add a Portal Linkset

Add New Linkset

VPN:	1
Id:	2
Name:	
Text:	
Autorun:	false

7. **In the Name field, enter a name for the linkset.**

   In this example we will call the linkset `EACA_passed`. This is a mandatory field.

8. **In the Text field, enter the linkset text.**

   The linkset text should read “`The Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent checks. No links will be configured for this linkset.

9. **Click Update.**

   The Portal Linksets form is redisplayed with the new linkset.

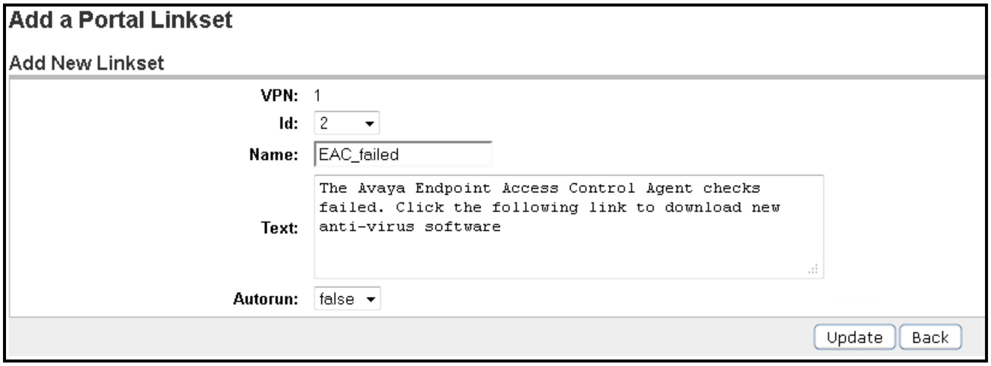
10. **Click Add to define a new linkset.**

    This linkset should print the result of the Avaya Endpoint Access Control Agent checks when they fail.

11. **In the Name field, enter the name `EACA_failed`.**

12. **In the Text field, enter the linkset text.**

    The linkset text should read “`The Avaya Endpoint Access Control Agent checks failed. Click the following link to download new anti-virus software.`”.



Add a Portal Linkset

Add New Linkset

VPN:	1
Id:	2
Name:	EAC_failed
Text:	The Avaya Endpoint Access Control Agent checks failed. Click the following link to download new anti-virus software
Autorun:	false

13. **Click Update.**

Configure a Link

The `EACA_failed` linkset should also contain a link to a web site where a new anti-virus program can be downloaded.

1. **Logon to the BBI as administrator.**

2. **Click Config tab.**

3. **Select VPN Gateways.**

   VPN Gateways form is displayed.

4. **Select the name of the VPN Gateway.**

5. **Select Linkset.**

   The Portal Links form is displayed.

6. **In the VPN Number and Portal Linkset list boxes, select the desired VPN and the portal linkset where the link should be included (that is, `EACA_failed`).**

7. **Click Refresh.**

8. **Click Add.**

   The Add Portal Links form is displayed.

9. **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`”.

10. **In the Link Type list box, select Internal Website as link type.**
11. **Click Continue.**

    The form is expanded.

12. **Under Internal Link Settings, in the Protocol list box, select `http`.**
13. **In the Host field, enter the address of the anti-virus program download site, e.g. `antivirus.example.com`.**
14. **In the Path field, enter a forward slash to imply the web server’s root or specify the desired path, e.g. `/update/file.html`.**
15. **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. **Logon to the BBI as administrator.**
2. **Click Config tab.**
3. **Select VPN Gateways.**

   VPN Gateways form is displayed.

4. **Select the VPN Gateway name.**
5. **Under settings, select Authorization.**
6. **Select Networks.**

   The Networks form is displayed.

7. **Click Add.**

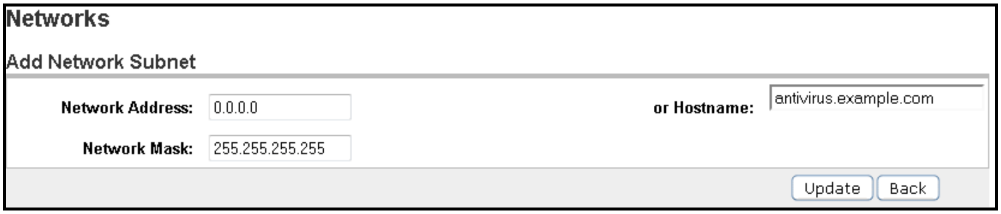
   The Add Network form is displayed.

8. **In the Name field, enter a name for the network, for example anti-virusweb.**
9. **Click Continue.**

   The form is expanded.

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

The Add Network Subnet form is displayed.



Networks

Add Network Subnet

Network Address:	0.0.0.0	or Hostname:	antivirus.example.com
Network Mask:	255.255.255.255		

11. **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.

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 Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent 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 Chapter 8, "Groups, Access Rules and Profiles".

1. **Logon to the BBI as administrator.**
2. **Click Config tab.**
3. **Select VPN Gateways.**

   VPN Gateways form is displayed.
4. **Select the name of the VPN Gateway.**
5. **Under settings, select Groups.**
6. **Click Add.**

   The Add New Group form is displayed.
7. **In the Name field, enter a name for the group, for example staff.**
8. **In the User Type list box, select novice.**
9. **Click Update.**
10. **In the System tree view select VPN Gateways.**
11. **Select the VPN Gateway name.**
12. **Under Settings, select EACA.**
13. **Select SRS Rules.**

    The SRS Rules form is displayed.
14. **To configure SRS Rules click on Launch button.**

NOTE – For information about configuring SRS Rules, see section "Avaya Endpoint Access Control Agent SRS Rules" on page 447.

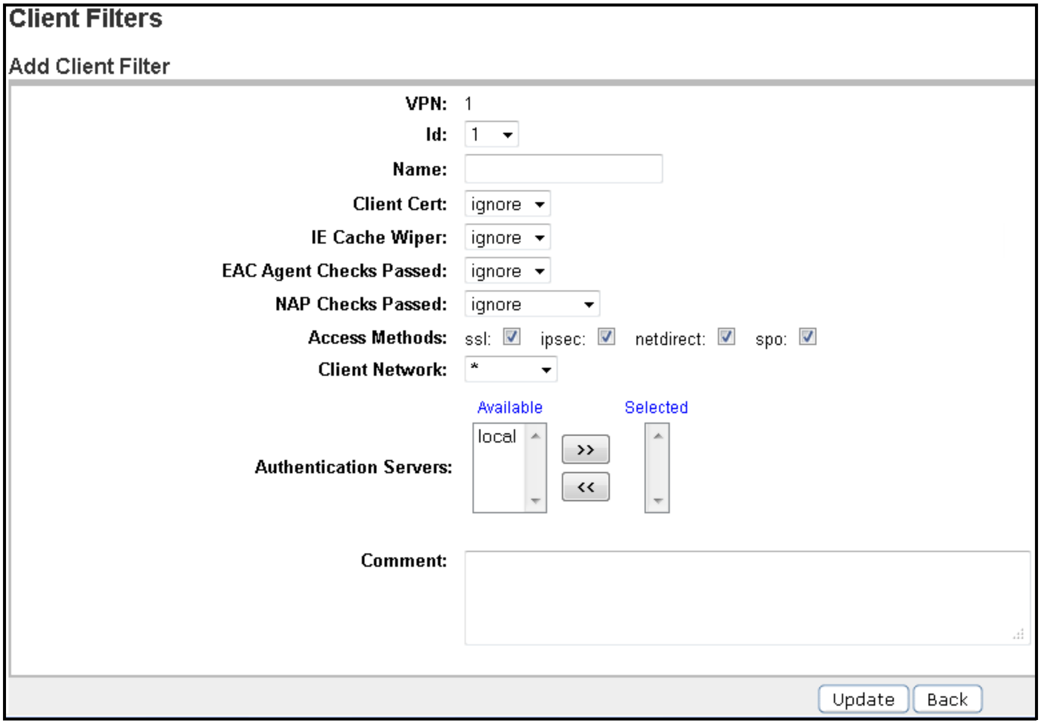
Create Client Filters

Two client filters need to be created. The first client filter should be triggered when the Avaya Endpoint Access Control Agent checks succeed. The other client filter should be triggered when the Avaya Endpoint Access Control Agent checks fail.

1. **Logon to the BBI as administrator.**
2. **Click Config tab.**
3. **Select VPN Gateways.**

   VPN Gateways form is displayed.
4. **Select the name of the VPN Gateway.**
5. **Under Settings, select Authorization.**
6. **Click Filters tab.**

7. **Click Add to add a client filter.**



Client Filters

Add Client Filter

VPN: 1

Id: 1

Name:

Client Cert: ignore

IE Cache Wiper: ignore

EAC Agent Checks Passed: ignore

NAP Checks Passed: ignore

Access Methods: ssl: ☑ ipsec: ☑ netdirect: ☑ spo: ☑

Client Network: *

Authentication Servers: Available: local Selected:

Comment:

8. **In the Name field, enter the name EACA_passed.**

9. **In the Avaya Endpoint Access Control Agent Checks Passed list box, select true.**

   This will trigger the client filter when the Avaya Endpoint Access Control Agent checks succeed.

10. **Select the tunneling protocol(s) used for the connection.**

    Several methods can be selected. Available methods are: ssl, ipsec, spo and netdirect.

11. **Click Update.**

    The Client Filters form is displayed with the newly created client filter.

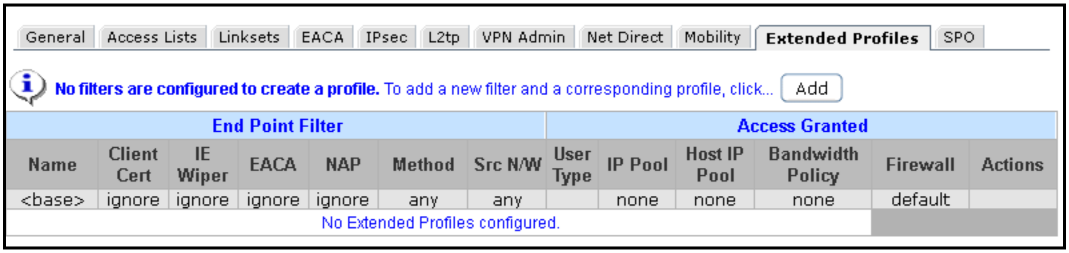
Configure Extended Profiles

Two extended profiles need to be created. The first profile should be triggered when the Avaya Endpoint Access Control Agent checks succeed. The second profile should be triggered when the Avaya Endpoint Access Control Agent checks fail.

1. **Logon to the BBI as administrator.**
2. **Click Config tab.**
3. **Select VPN Gateways.**

   VPN Gateways form is displayed.
4. **Select the name of the VPN Gateway.**
5. **Under settings, select Groups.**
6. **Select the Group name.**
7. **Select Extended Profiles.**

   Extended Profiles form is displayed.



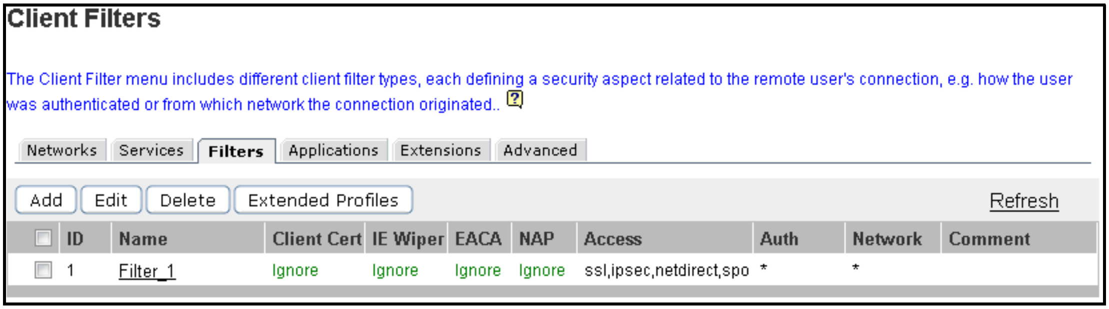
No filters are configured to create a profile. To add a new filter and a corresponding profile, click...

End Point Filter							Access Granted					
Name	Client Cert	IE Wiper	EACA	NAP	Method	Src N/W	User Type	IP Pool	Host IP Pool	Bandwidth Policy	Firewall	Actions
<base>	ignore	ignore	ignore	ignore	any	any		none	none	none	default	
No Extended Profiles configured.												

8. **Click on Add button.**

   Client filters and extended profiles are automatically added to the database.

9. **If you want to view only the client information, then click on End Point Filter link.**



Client Filters

The Client Filter menu includes different client filter types, each defining a security aspect related to the remote user's connection, e.g. how the user was authenticated or from which network the connection originated..

□	ID	Name	Client Cert	IE Wiper	EACA	NAP	Access	Auth	Network	Comment
□	1	Filter_1	Ignore	Ignore	Ignore	Ignore	ssl,ipsec,netdirect,spo	*	*	

10. **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 is displayed.

2. **Select the name of the VPN Gateway.**

3. **Under settings, select Groups.**

4. **Select the name of the VPN Gateway.**

5. **Under settings, select Groups.**

6. **Select the Group name.**

7. **Select Extended Profiles.**

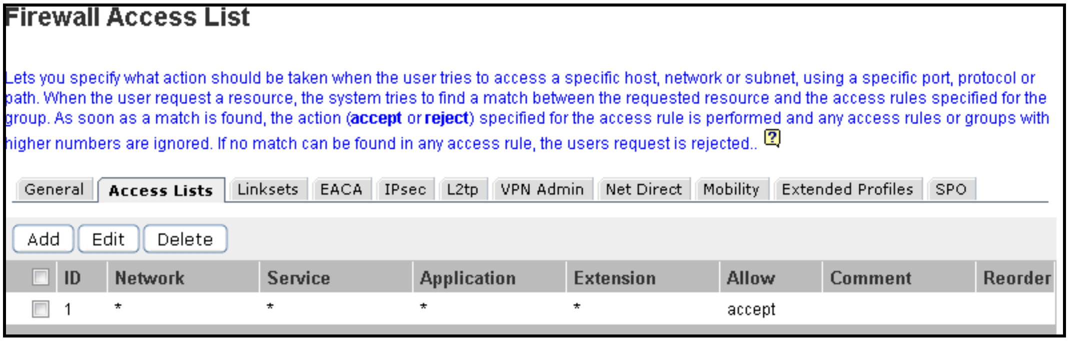
   Extended Profiled form is displayed.

8. **Click on Add button.**

   Client filters and extended profiles are automatically added to the database.

9. **Under Actions column in the table, click on the modify link.**

10. **Click on Access Lists tab.**



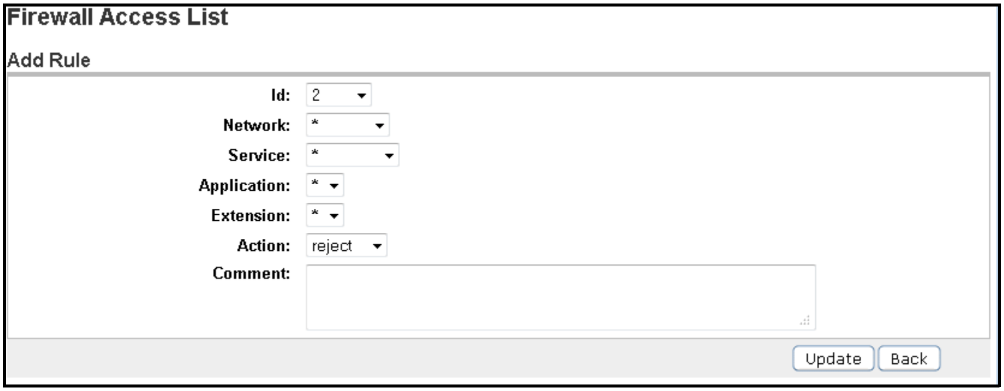
Firewall Access List

Lets you specify what action should be taken when the user tries to access a specific host, network or subnet, using a specific port, protocol or path. When the user request a resource, the system tries to find a match between the requested resource and the access rules specified for the group. As soon as a match is found, the action (**accept** or **reject**) specified for the access rule is performed and any access rules or groups with higher numbers are ignored. If no match can be found in any access rule, the users request is rejected..

□	ID	Network	Service	Application	Extension	Allow	Comment	Reorder
□	1	*	*	*	*	accept		

11. **Click Add.**

The Add Rule form is displayed.



Firewall Access List

Add Rule

Id:	2
Network:	*
Service:	*
Application:	*
Extension:	*
Action:	reject
Comment:	

12. **Keep the asterisks (*) in the Network, Service and Application list boxes. This implies all networks, port numbers, protocols and paths.**

13. **In the Action list box, select Accept.**

14. **Click Update.**

    The Extended Access List form is redisplayed. The next step is to create the access rules for the second extended profile.

15. **In the Client Filter list box, select `EACA_failed`.**

16. **Click Refresh.**

17. **Click Add.**

    The Add Rule form is displayed.

18. **In the Network list box, select the network definition we created in the section** “Configure a Network” on page 473**, that is,**
    `anti-virusweb`.

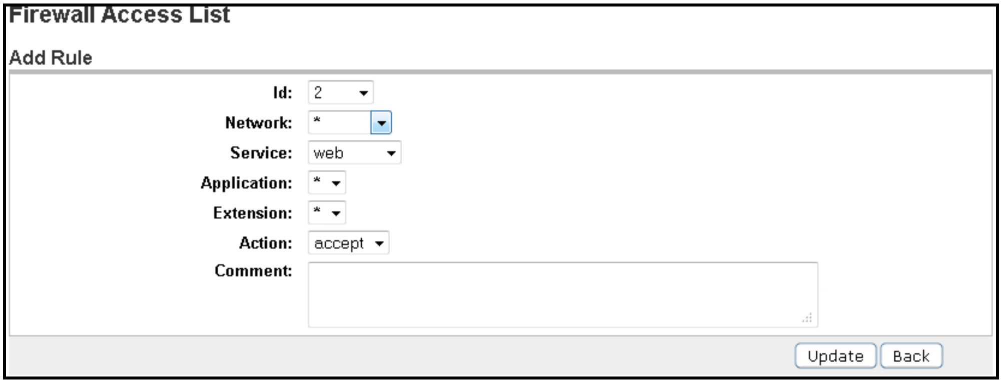
    This limits access to the web site where the anti-virus program can be downloaded.

19. **In the Service list box, select `web`.**

    This limits access to the FTP, HTTP and HTTPS protocols.

20. **Keep the asterisk (*) in the Application list box. This implies all paths.**

21. **In the Action list box, select Accept.**



Firewall Access List

Add Rule

Id: 2

Network: *

Service: web

Application: *

Extension: *

Action: accept

Comment:

22. **Click Update.**

Now that the access rules are configured, we should also map the linksets that were created in section "Configure Linksets" on page 470 to the extended profiles.

Map Linksets to Extended Profiles

1. **In the system tree view, select VPN Gateways.**

   VPN Gateways form is displayed.

2. **Select the name of the VPN Gateway.**

3. **Under settings, select Groups.**

4. **Select the name of the VPN Gateway.**

5. **Under settings, select Groups.**

6. **Select the Group name.**

7. **Select Extended Profiles.**

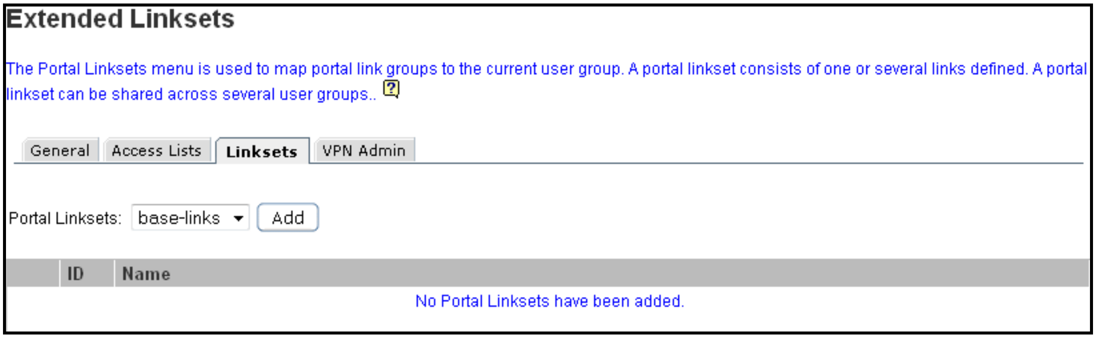
   Extended Profiled form is displayed.

8. **Click on Add Profile button.**

   Client filters and extended profiles are automatically added to the database.

9. **Under Actions column in the table, click on the modify link.**

10. **Click on Linksets tab.**



Extended Linksets

The Portal Linksets menu is used to map portal link groups to the current user group. A portal linkset consists of one or several links defined. A portal linkset can be shared across several user groups..

Portal Linksets: base-links Add

ID	Name
No Portal Linksets have been added.	

11. **In the Portal Linksets list box, select the linkset.**

12. **Click Add.**

    This maps the linkset to the extended profile.

13. **In the Client Filter list box, select the second client filter (extended profile), that is, `EACA_failed`.**

14. **Click Refresh.**

15. **In the Portal Linksets list box, select the linkset `EACA_failed`.**

    This linkset also contains a link that directs the remote user to the anti-virus program download site.

16. **Click Add.**

    This maps the linkset `EACA_failed` to the extended profile `EACA_failed`.

17. **Apply the changes.**

    For more instructions on how to create groups, access rules and profiles, see Chapter 8, “Groups, Access Rules and Profiles”.

Test the Example Configuration

To test how Avaya Endpoint Access Control Agent behaves when configured as described in the previous example, proceed as follows:

1. **In your browser, enter the IP address or domain name to the desired VPN.**

   The Portal login page is displayed.

2. **Log in to the Portal.**

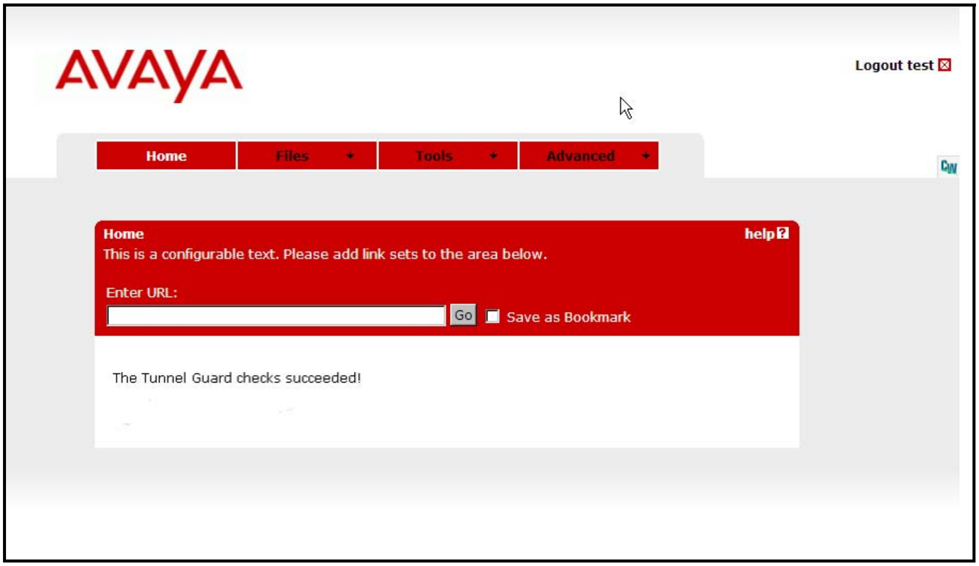
   This example assumes that you have configured a user that belongs to the `staff` group. For instructions on how to add users to the local database, see Chapter 9, "Authentication Methods".

   The Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent checks fail. The result is displayed on the Portal page.

Avaya Endpoint Access Control Agent Checks Succeeded

This is what the Portal page might look like if the Avaya Endpoint Access Control Agent checks succeeded, that is, the requested anti-virus software was present on the client PC.



Home

This is a configurable text. Please add link sets to the area below.

Enter URL: □ ☐ Save as Bookmark

The Tunnel Guard checks succeeded!

To confirm that Avaya Endpoint Access Control Agent is running and that the checks have succeeded, the Avaya Endpoint Access Control Agent Success icon is displayed to the right of the Portal tabs (for an explanation of the other icons, see Chapter 6, “The Portal from an End-User Perspective”).

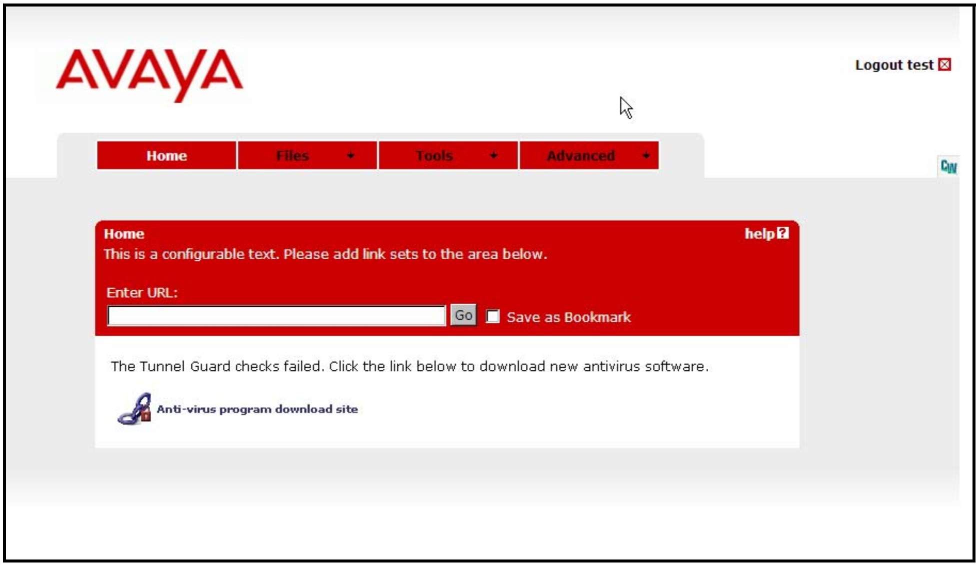
The client filter called `EACA_passed` triggered when the Avaya Endpoint Access Control Agent checks succeeded. This in its turn triggered Extended profile 1 (`EACA_passed`) in the `staff` group, because Extended profile 1 references the client filter `EACA_passed`.

The linkset used in Extended profile 1 is a linkset called `EACA_passed`. It has no links but prints the text “The Avaya Endpoint Access Control Agent 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

This is what the Portal page might look like if the Avaya Endpoint Access Control Agent checks failed, that is, the requested anti-virus software was *not* present on the client machine.



Home

This is a configurable text. Please add link sets to the area below.

Enter URL:

The Tunnel Guard checks failed. Click the link below to download new antivirus software.

Anti-virus program download site

To confirm that Avaya Endpoint Access Control Agent is running but the checks have failed, the Avaya Endpoint Access Control Agent Failure icon is displayed to the right of the Portal tabs (for an explanation of the other icons, see Chapter 6, "The Portal from an End-User Perspective").

The client filter called `EACA_failed` triggered when the Avaya Endpoint Access Control Agent checks failed. This in turn triggered Extended profile 2 (`EACA_failed`) in the `staff` group, because Extended profile 2 references the client filter `EACA_failed`.

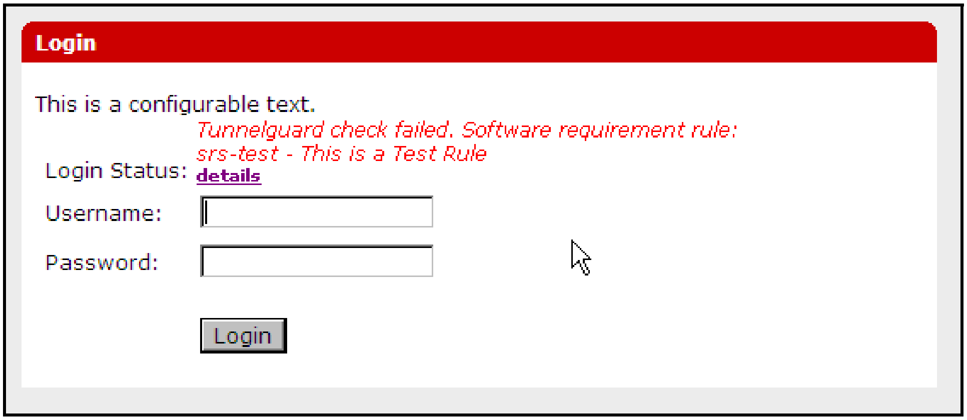
The linkset used in Extended profile 2 is a linkset called `EACA_failed`. It prints the text "The Avaya Endpoint Access Control Agent checks failed. Click the following link to download new anti-virus software". The linkset includes one link, directing the user to an anti-virus program download site.

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 Avaya Endpoint Access Control Agent operates in `restricted` mode. The user is logged in to the Portal but access is restricted.

If Avaya Endpoint Access Control Agent 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 Avaya Endpoint Access Control Agent check:



Login

This is a configurable text.

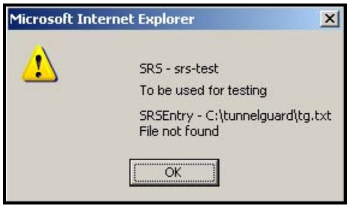
Login Status: *Tunnelguard check failed. Software requirement rule: srs-test - This is a Test Rule* details

Username:

Password:

The Avaya Endpoint Access Control Agent rule expression (srs-test) and the Avaya Endpoint Access Control Agent rule comment (This is a Test Rule) are automatically displayed. For a description of how to configure Avaya Endpoint Access Control Agent rule comments, see the section "Add Avaya Endpoint Access Control Agent Rule Message" on page 462.

When the user clicks the **details** link, a message window appears:



Microsoft Internet Explorer

SRS - srs-test

To be used for testing

SRSEntry - C:\tunnelguard\tg.txt
File not found

This window provides more detailed information about the failed Avaya Endpoint Access Control Agent 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 Predefined Software Definition Message" on page 463.

If desired, the **details** link can be hidden. Go to **VPN Gateways>VPN #>Avaya Endpoint Access Control Agent>Setup** and select `off` in the **Display SRS Failure Details** check box. This will also disable the `<var:eacFailureDetail>` variable.

CHAPTER 16
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 is displayed. If malicious code is detected, the offending process can be terminated, quarantined and reported.

Configuration

The configuration on the Avaya VPN Gateway 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 Avaya VPN Gateway and the WholeSecurity server. IP addresses do not work.
- The Avaya VPN Gateway 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 Avaya VPN Gateway 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 Avaya VPN Gateway and WholeSecurity servers should be in the same domain. For example, if the Avaya VPN Gateway is `vpn.example.com`, the WholeSecurity server should also reside in the `example.com` domain, for example as `ws.example.com`.

Configure a Deployment in WholeSecurity

Before you start configuring the Avaya VPN Gateway, 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 Avaya VPN Gateway needs to access scripts in this directory to check the scan results, you must add the Avaya VPN Gateway’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

The following sections describe each step of the configuration required on the Avaya VPN Gateway. A quicker way of making the same settings is to run the WholeSecurity wizard (under **VPN Gateways>VPN #>WholeSecurity>General (WholeSecurity Quick Wizard)**). Refer to the following sections for examples of information to be supplied in the wizard.

1. **Logon to the BBI as administrator.**

2. **Click Config tab.**

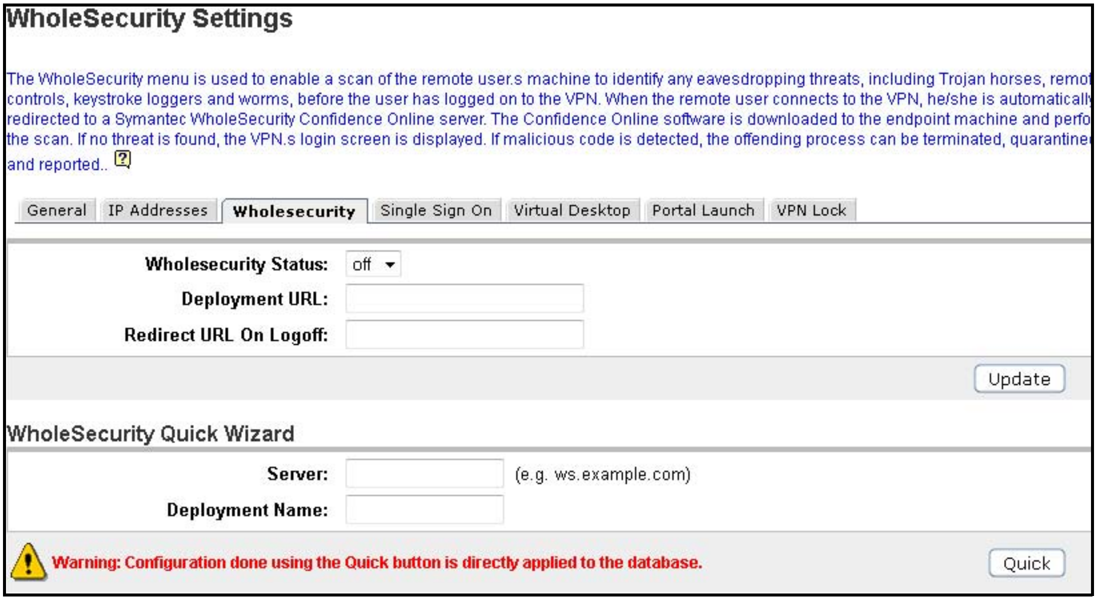
3. **Select VPN Gateways.**

   VPN Gateways form is displayed.

4. **Select the name of the VPN Gateway.**

5. **Under settings, select General.**

6. **Select Wholesecurity.**



WholeSecurity Settings

The WholeSecurity menu is used to enable a scan of the remote user.s machine to identify any eavesdropping threats, including Trojan horses, remot controls, keystroke loggers and worms, before the user has logged on to the VPN. When the remote user connects to the VPN, he/she is automaticall redirected to a Symantec WholeSecurity Confidence Online server. The Confidence Online software is downloaded to the endpoint machine and perfo the scan. If no threat is found, the VPN.s login screen is displayed. If malicious code is detected, the offending process can be terminated, quarantine and reported..

Wholesecurity Status: off

Deployment URL:

Redirect URL On Logoff:

WholeSecurity Quick Wizard

Server: (e.g. ws.example.com)

Deployment Name:

Warning: Configuration done using the Quick button is directly applied to the database.

7. **In the Status list box, select on.**

8. **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 would be:

```
https://ws.example.com/llclient/SSLVPN/online.html
```

9. **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.

10. **Click Update.**

11. **Specify the WholeSecurity server name.**

12. **Specify the WholeSecurity Deployment name.**

13. **Click Quick to configure the WholeSecurity settings for the current VPN with the values specified.**

14. **Click Apply to 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.

This network definition should later be referenced in the anonymous group’s access rules.

1. **Logon to the BBI as administrator.**

2. **Click Config tab.**

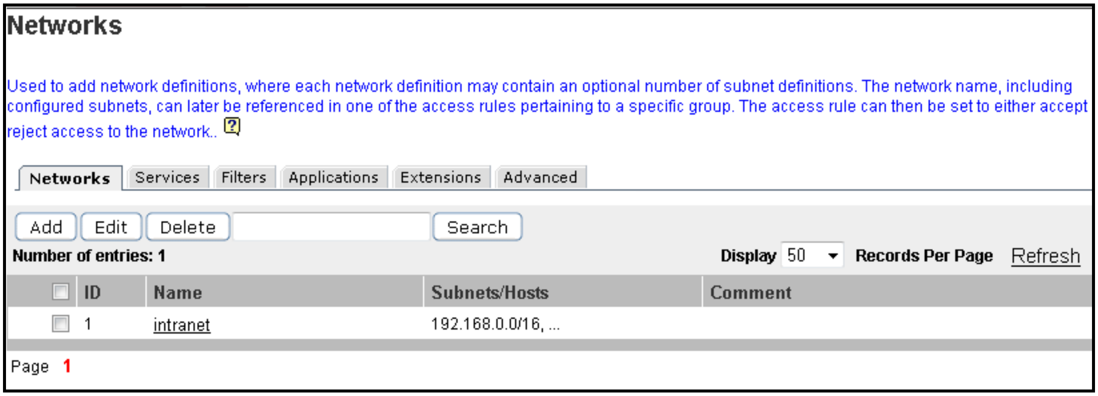
3. **Select VPN Gateways.**

   The VPN Gateways form appears.

4. **Select the name of the VPN Gateway.**

5. **Under settings, select Authorization.**

   The Networks form is displayed.



Networks

Used to add network definitions, where each network definition may contain an optional number of subnet definitions. The network name, including configured subnets, can later be referenced in one of the access rules pertaining to a specific group. The access rule can then be set to either accept reject access to the network..

Number of entries: 1

Display 50 Records Per Page Refresh

	ID	Name	Subnets/Hosts	Comment
□	1	intranet	192.168.0.0/16, ...	

Page 1

We will create a network definition corresponding to the WholeSecurity Confidence Online server.

6. **Click Add.**

   The Add Network form is displayed.

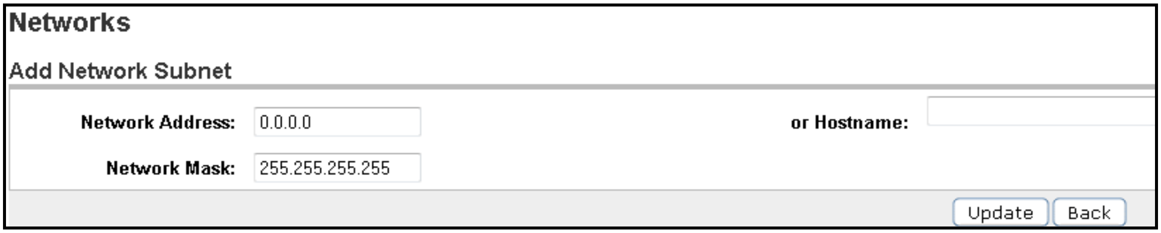
7. **In the Name field, enter a name for the network definition, for example wholesecurity.**

8. **Click Continue.**

   The form is expanded with the Network Subnet subform.

9. **Click Add to add a new subnet.**

   The Add Network Subnet form is displayed.



Networks

Add Network Subnet

Network Address: 0.0.0.0

or Hostname:

Network Mask: 255.255.255.255

10. **In the Hostname field, enter the name of the Confidence Online server**

    This could for example be ws.example.com.

11. **Click Add.**

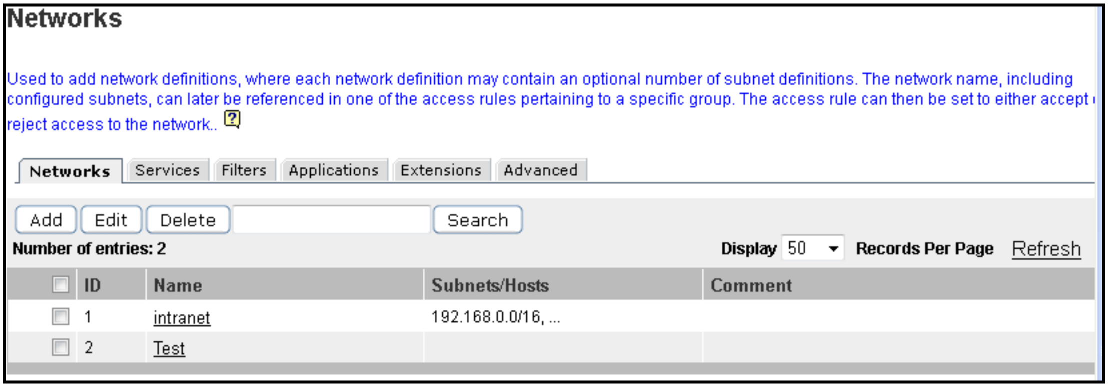
12. **Select VPN Gateways.**

The VPN Gateways form appears.

13. **Select the name of the VPN Gateway.**

14. **Under settings, select Authorization.**

The network should now be added to the list of network definitions.



Networks

Used to add network definitions, where each network definition may contain an optional number of subnet definitions. The network name, including configured subnets, can later be referenced in one of the access rules pertaining to a specific group. The access rule can then be set to either accept reject access to the network..

Number of entries: 2

Display 50 Records Per Page

□	ID	Name	Subnets/Hosts	Comment
□	1	intranet	192.168.0.0/16, ...	
□	2	Test		

15. **Apply the changes.**

Configure an Appspec Definition

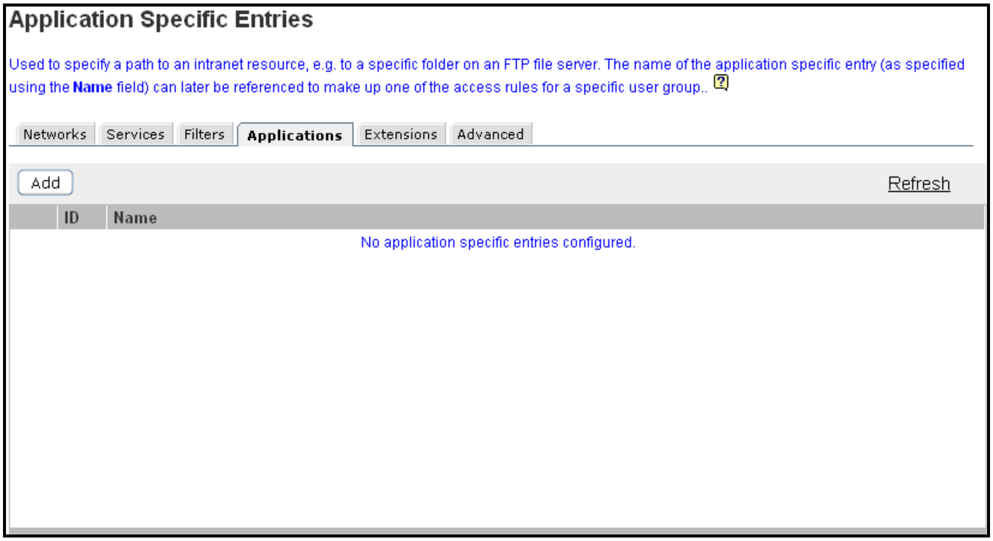
By specifying an application specific (appspec) definition identifying specific paths, you can limit the user’s access rights on the WholeSecurity Confidence Online server.

This appspec definition should later be referenced in the anonymous group’s access rules.

1. **Logon to the BBI as administrator.**
2. **Click Config tab.**
3. **Select VPN Gateways.**

   The VPN Gateways form appears.
4. **Select the name of the VPN Gateway.**
5. **Under settings, select Authorization.**
6. **Select Applications.**

   The Applications Specific Entries form is displayed.



Application Specific Entries

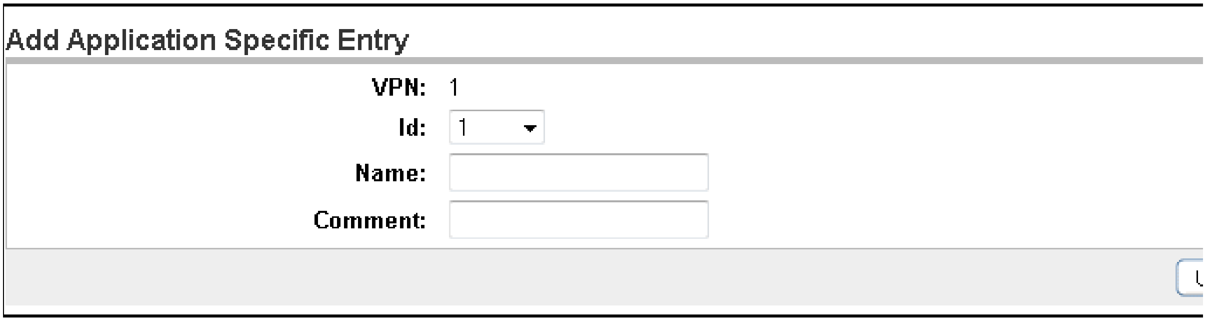
Used to specify a path to an intranet resource, e.g. to a specific folder on an FTP file server. The name of the application specific entry (as specified using the **Name** field) can later be referenced to make up one of the access rules for a specific user group..

ID	Name

No application specific entries configured.

7. **Click Add.**

   The Add Application Specific Entry form is displayed.



Add Application Specific Entry

VPN:	1
Id:	1
Name:	
Comment:	

8. **In the Name field, enter the name of the appspec entry, for example wholesecurity.**

9. **Click Update.**

10. **In the system tree view, select VPN Gateways.**

    The VPN Gateways form appears.

11. **Select the name of the VPN Gateway.**

12. **Under settings, select Authorization.**

13. **Select Applications.**

    The General form is displayed.

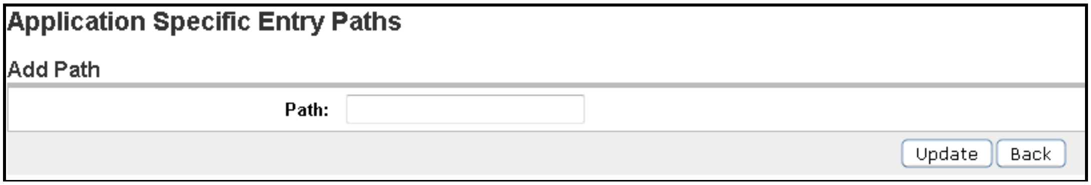
14. **Go to Application Entry Paths.**

    The Application Specific Entry Paths form appears.

15. **Click Add.**

    The Add Path form is displayed.

16. **In the Path field, enter the first path, i.e. /cgi-bin/rr.fcgi.**



Application Specific Entry Paths

Add Path

Path:	

17. **Click Update.**

The path is added to the Application Specific Entry Paths form.

18. **Click Add to add a second path.**

    The Add Path form is displayed.

19. **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.

20. **Click Update.**

    The Application Specific Entry Paths form is redisplayed with the second path added.

21. **Apply the changes.**

Configure an Anonymous Group

1. **Logon to the BBI as administrator.**

2. **Click Config tab.**

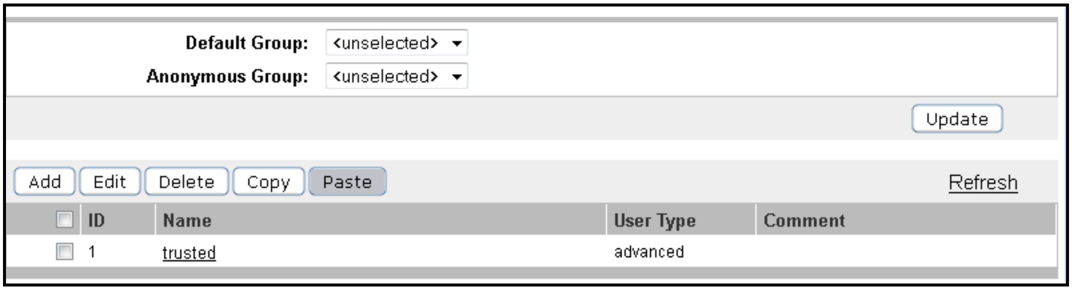
3. **Select VPN Gateways.**

   The VPN Gateways form appears.

4. **Select the name of the VPN Gateway.**

5. **Under settings, select Groups.**

   The Groups form appears.



Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

6. **Click Add.**

   The Add New Group form is displayed.

7. **In the Name field, enter a name for the group, for example wholesecurity.**

8. **Click Update.**

   The Groups form is redisplayed with the new group added to the list.

9. **Under settings, select Groups.**

10. **Select Access List.**

    The Firewall Access List Form is displayed.

11. **Click Add.**

    The Add Rule form is displayed.

    In the Network list box, select the network definition called wholesecurity.

    This is the network definition created in the section "Configure a Network Definition" on page 492. By referencing this network in the access rule, access will be granted to the Confidence Online server and nothing else.

12. **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 177).

    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 495. 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.

13. **In the Action list box, select Accept.**

14. **Click Update.**

15. **Under settings, select Groups.**

    The Groups form is displayed

16. **In the Anonymous Group list box, select wholesecurity.**

    The final step is to make the group we just created an anonymous group.

17. **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 17
Secure Service Partitioning

The Avaya VPN Gateway software provides the ability to partition a cluster of Avaya VPN Gateways into separate VPNs. The idea is to give service providers (ISPs) the possibility to host multiple VPN customers on a shared Remote Access Services (RAS) platform.

The high-level capabilities include:

- Multiple domains. The ability to host up to 1024 public termination points for end-customer SSL and IPsec VPNs.
- Secure VPN binding. Each VPN is bound to a private IP interface. VLAN tagging can be used when private IP address spaces overlap.
- Private network authentication. Existing authentication servers within the customer's private network are used.
- Access control. Unique access rules can be specified for each user group in the various VPNs.
- Private network name resolution. If desired, private network DNS servers can be mapped to the VPN.
- Split administration. VPN management is enabled for each VPN customer through a web interface, without exposing global administration access.
- High availability. The Secure Service Partitioning (SSP) solution is compatible with the Avaya VPN Gateway cluster's high availability solutions.

This chapter describes the steps required to set up a basic SSP solution, in this case two Avaya VPN Gateway Portals, each of which is bound to a private network.

For an overview of all other steps required for a fully functional SSP solution, see Chapter 5, "Clientless Mode".

802.1Q VLAN Tags

Access to private customer networks can be enabled through 802.1Q VLAN tags. The Avaya VPN Gateway platform will connect to a device that can direct traffic to the appropriate private side network based on 802.1Q tags. These private networks may actually be a member of a site-to-site VPN using MPLS, IPsec, L2 Optical Ethernet or any other VPN technology as long as the device connected to the Avaya VPN Gateway platform can direct traffic to/from these VPNs based on 802.1Q VLAN tags.

Where functionality is concerned, there is no difference between using VLAN tagged interfaces or physical interfaces. For small setups, it is fully possible to use the physical interfaces (that is, ports) to split two VPNs. It is likewise possible to VLAN tag only some of the interfaces.

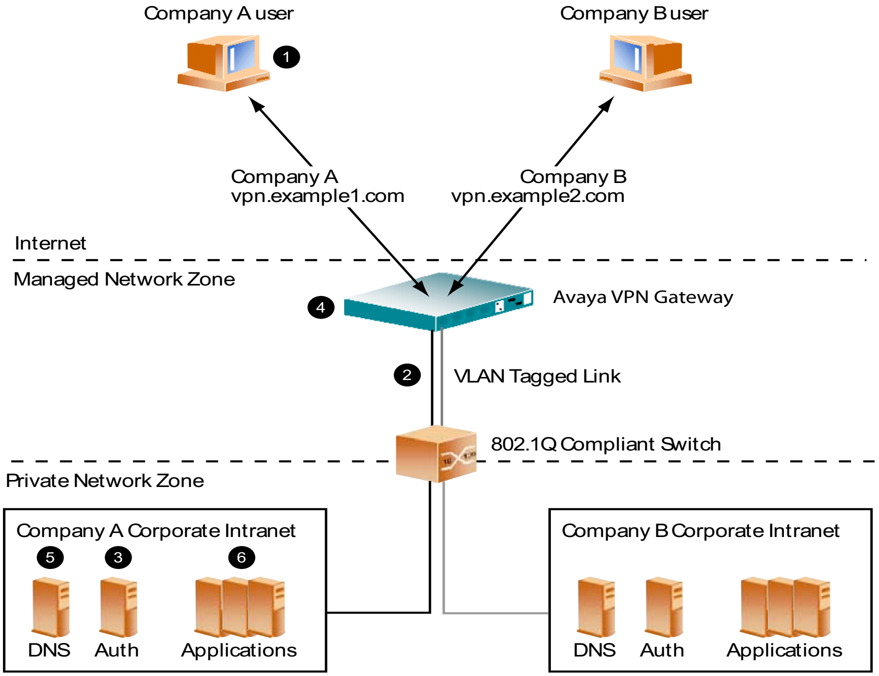
License Keys

To enable the Secure Service Partitioning feature in the Avaya VPN Gateway software, a license key must be obtained from Avaya. This also the case if you wish to enable SSL or IPsec access for more than 50 concurrent users. To obtain the license keys, you have to provide the MAC address of each Avaya VPN Gateway for which a license should be installed.

For instructions on how to obtain the MAC address and how to paste the license key, see “Licenses” on page 73 in Chapter 4, “VPN Introduction”.

Connection Example

1. A user from Company A browses to **https://vpn.example1.com** from the Internet. This DNS domain name points to a virtual address on the Avaya VPN Gateway's traffic interface. The appropriate SSL certificate is presented for the Company A Portal. A custom login screen is presented. The user provides appropriate login credentials which are validated using any of the supported authentication schemes such as RADIUS, LDAP, NTLM or RSA SecurID.
2. All connections from the Company A Portal are bound to a specific interface (may be VLAN tagged) on the private/internal side.
3. In this example the authentication server is located inside Company A's corporate Intranet.
4. After validating the login credentials, the user is bound to a user-group based on the response from the authentication server. This group will determine access rules for the user and restrict access to certain resources within the private network. The custom Company A Portal is presented including only the application links applicable for this user.
5. As the user selects application links from the Portal, the Avaya VPN Gateway will query the private DNS server to resolve host names into IP addresses.
6. The user will access applications within the private network zone.



Configuration Example

In this example we will create two unique VPN Portal configurations on a single Avaya VPN Gateway platform. These two independent customer Portals will link to two respective private networks in a secure fashion such that the first Portal will not provide access to the second internal network and vice versa.

This example will use completely overlapping IP addresses to demonstrate support for this topology. Any customer network subnets can be used as appropriate.

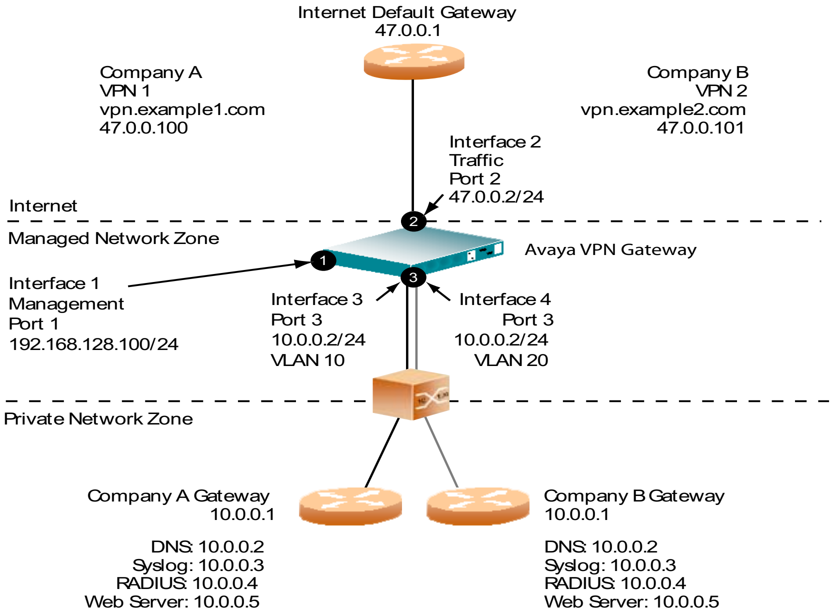


Figure 17-1 Two VPNs on a Single AVG Platform

Initial Setup

Before you can start configuring the VPNs you should perform an initial setup of the system. The initial setup procedure is described in the “Initial Setup” chapter in the *User's Guide*.

Configure the Interfaces

As shown in Figure 17-1, four interfaces are required to configure the two VPNs.

Check the Settings for Interface 1

When you ran the initial setup, Interface 1 was created as the management interface, that is, on the private or internal side (not facing the Internet) of the Avaya VPN Gateway. If you need to view or edit the settings for Interface 1, follow the following steps.

1. **Log on to the BBI as administrator.**

2. **In the System tree view, select Host(s).**

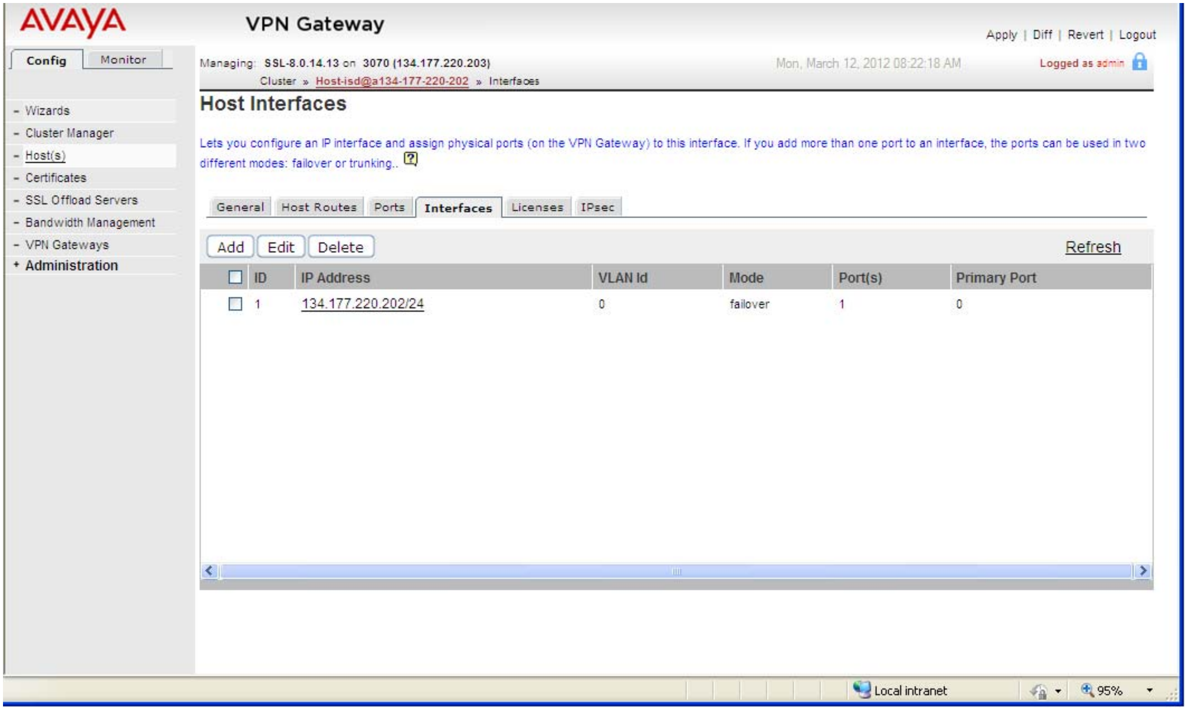
   The VPN Gateway Host(s) form is displayed.

3. **In SSL-VPN Host(s), in the Hostname field, select the VPN Gateway for which you wish to configure a new interface.**

   The System Information form is displayed.

4. **Select Interfaces.**

   The Host Interfaces form is displayed with configured interfaces for the current host (VPN Gateway).



Managing: SSL-8.0.14.13 on 3070 (134.177.220.203)   Mon, March 12, 2012 08:22:18 AM   Logged as admin

Cluster » Host-isd@a134-177-220-202 » Interfaces

Host Interfaces

Lets you configure an IP interface and assign physical ports (on the VPN Gateway) to this interface. If you add more than one port to an interface, the ports can be used in two different modes: failover or trunking..

□	ID	IP Address	VLAN Id	Mode	Port(s)	Primary Port
□	1	134.177.220.202/24	0	failover	1	0

Verify that the management interface on the “private” or “internal” side of the Avaya VPN Gateway has the correct IP address and network mask. Also verify that this interface uses the desired physical port on the Avaya VPN Gateway (displayed under Port(s).

5. **In the System Information form, select General. The Default Gateway Address form is displayed.**

   You had the option to configure a default gateway during the initial setup. Verify that the default gateway is assigned the correct IP address.

   To edit the current gateway setting, enter the desired IP address and click Update.

NOTE – The default gateway must always reside on the traffic interface, that is, on the public or external side (facing the Internet).

In the next steps, configure the traffic interface.

Configure Interface 2

During the initial setup you may have configured Interface 2 as well, if you chose to set up a two-armed configuration. This instruction assumes that Interface 2 has not yet been configured.

1. **In the System tree view, select Host(s).**

   The VPN Gateway Host(s) form is displayed.

2. **In SSL-VPN Host(s), in the Hostname field, select the VPN Gateway for which you wish to configure a new interface.**

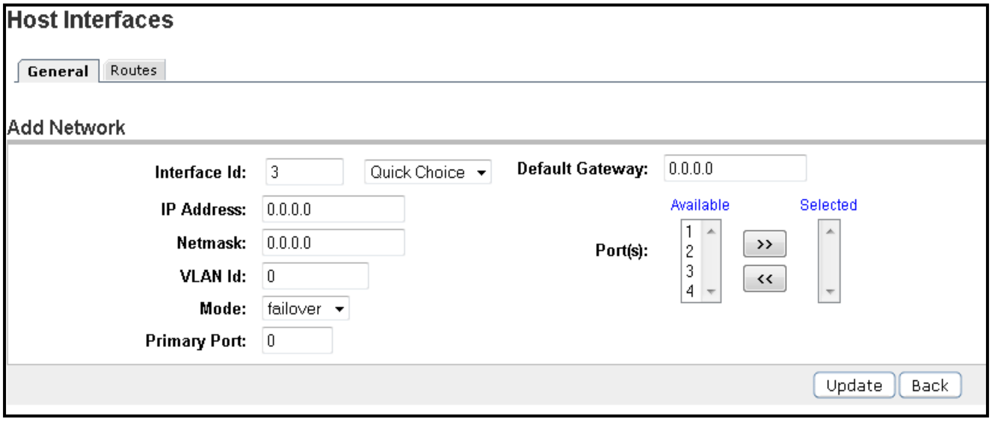
   The System Information form is displayed.

3. **Select Interfaces.**

   The Host Interfaces form is displayed with configured interfaces for the current host (VPN Gateway).

4. **Click Add.**

The Add Network form is displayed.



Interface Id: 3

Default Gateway: 0.0.0.0

IP Address: 0.0.0.0

Netmask: 0.0.0.0

VLAN Id: 0

Mode: failover

Primary Port: 0

Port(s): Available: 1, 2, 3, 4; Selected:

The new interface is assigned number 2 in the Id field.

5. **In the Address and Netmask field, configure Interface 2 with an IP address and network mask.**

   In this example we will use the IP address `47.0.0.2` and the network mask `255.255.255.0`. This IP address should be used by the traffic interface on the “public” or “external” side (facing the Internet) of the Avaya VPN Gateway.

6. **In the Ports list, under Available, select port 2 and click >> to move the item to the Selected list.**

   This binds the interface to port 2 on the Avaya VPN Gateway.

7. **Click Update.**

8. **Apply the changes.**

Configure Interface 3

This section describes how to configure interface 3, that is, the interface required for Company A’s private network zone.

1. **In the System tree view, select Host(s).**

   The VPN Gateway Host(s) form is displayed.

2. **In SSL-VPN Host(s), in the Hostname field, select the VPN Gateway for which you wish to configure a new interface.**

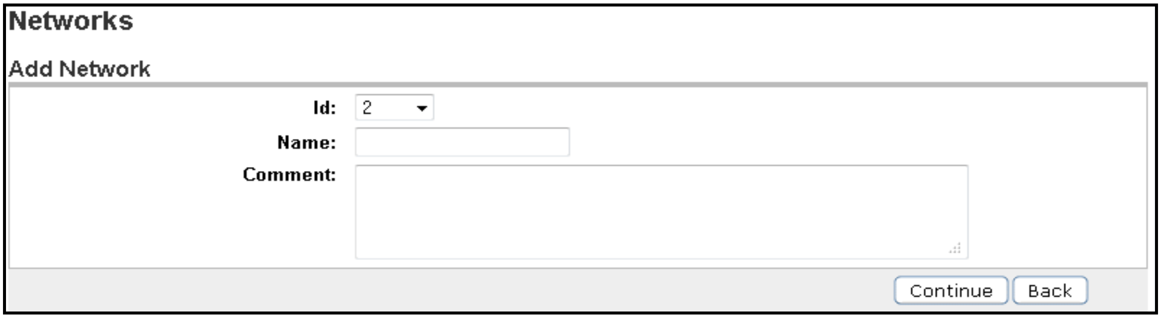
   The System Information form is displayed.

3. **Select Interfaces.**

   The Host Interfaces form is displayed with configured interfaces for the current host (VPN Gateway).

4. **Click Add.**

   The Add Network form is displayed.



Networks

Add Network

Id: 2

Name:

Comment:

5. **In the Address and Netmask field, configure Interface 3 with an IP address and network mask.**

   They should match the network required for Company A's private network zone, that is, 10.0.0.2/24 in this example.

6. **In the VLAN Id field, enter 10 as VLAN tag ID.**

7. **In the Ports list, under Available, select port 3 and click >> to move the item to the Selected list.**

   This binds the interface to port 3 on the VPN Gateway.

8. **In the Interface Id list box, select the interface for which you want to configure a default gateway.**

9. **In the Default Gateway list box, enter a default gateway address for Interface 3.**

   In this example, the default gateway for Interface 3 is configured as 10.0.0.1. This action routes all traffic bound for Company A's intranet to the default gateway.

   You also have an option to configure static routes for the backend (private side) traffic, under **Cluster> Hosts(s)>Interfaces>Routes.**

10. **Click Update.**

11. **Apply the changes.**

Configure Interface 4

This section describes how to configure interface 4, that is, the interface required for Company B's private network zone.

1. **In the System tree view, select Host(s). The VPN Gateway Host(s) form is displayed.**

2. **In SSL-VPN Host(s), in the Hostname field, select the VPN Gateway for which you wish to configure a new interface.**

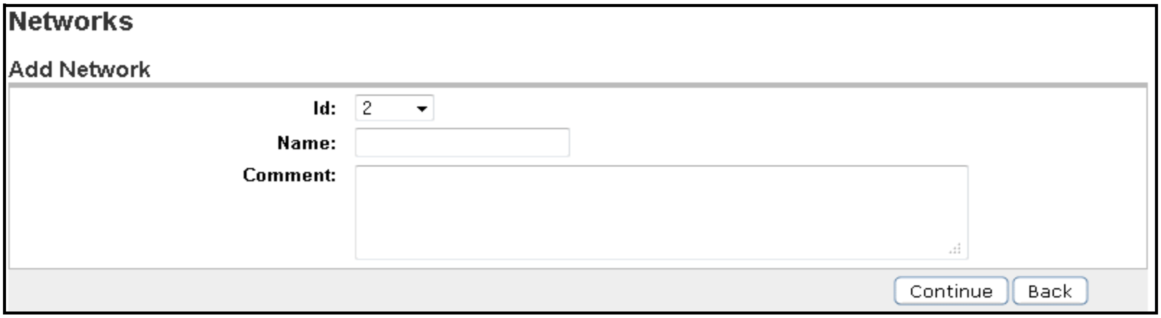
   The System Information form is displayed

3. **Select Interfaces.**

   The Host Interfaces form is displayed with configured interfaces for the current host (VPN Gateway).

4. **Click Add.**

   The Add Network form is displayed.



Networks

Add Network

Id: 2

Name:

Comment:

5. **In the Address and Netmask field, configure Interface 4 with an IP address and network mask.**

   They should match the network required for Company A's private network zone, that is, 10.0.0.2/24 in this example.

6. **In the VLAN Id field, enter 20 as VLAN tag ID.**

7. **In the Ports list, under Available, select port 3 and click >> to move the item to the Selected list.**

   This binds the interface to port 3 on the VPN Gateway.

8. **In the Interface Id list box, select the interface for which you want to configure a default gateway, that is, interface 4.**

9. **In the Default Gateway text box, enter a default gateway address for Interface 4.**

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

Configure VPN 1

In this example, two VPNs should be configured, one for Company A (VPN 1) and one for Company B (VPN 2).

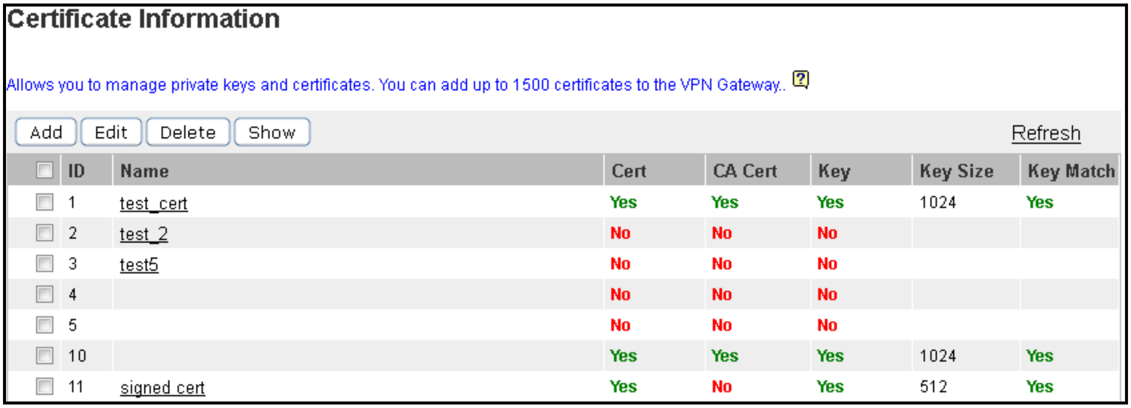
NOTE – If you run the Quick VPN setup wizard during the initial setup, VPN 1 has already been created. You can either edit the settings for VPN 1 to adapt it to the requirements of your customer or keep it as a test VPN for your own testing. This configuration example assumes that you have not yet created a VPN.

Import Signed Certificate to the Avaya VPN Gateway

This instruction assumes that you have a real server certificate available, signed by a CA authority. The certificate can be imported to the Avaya VPN Gateway as a file, through the BBI, or be pasted into the BBI as text.

1. **In the System tree view, select Certificates.**

   The test certificate created when you ran the VPN Quick setup wizard is displayed If you run the VPN Quick Setup wizard.



Certificate Information

Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		
□	4		No	No	No		
□	5		No	No	No		
□	10		Yes	Yes	Yes	1024	Yes
□	11	signed cert	Yes	No	Yes	512	Yes

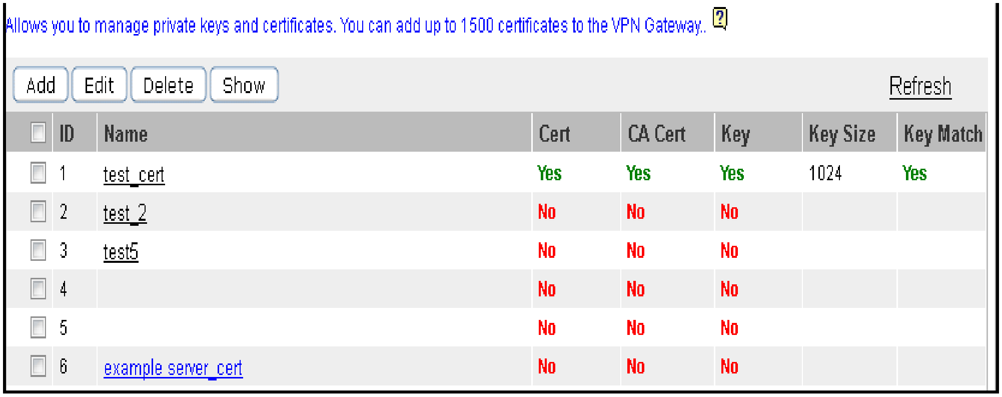
2. **Click Add.**

   The Add New Certificate form is shown. The new certificate is assigned certificate number 2.

3. **In the Name field, enter an appropriate name for the certificate, for example server_cert.**

4. **Click Update.**

A place holder for the new certificate is created.



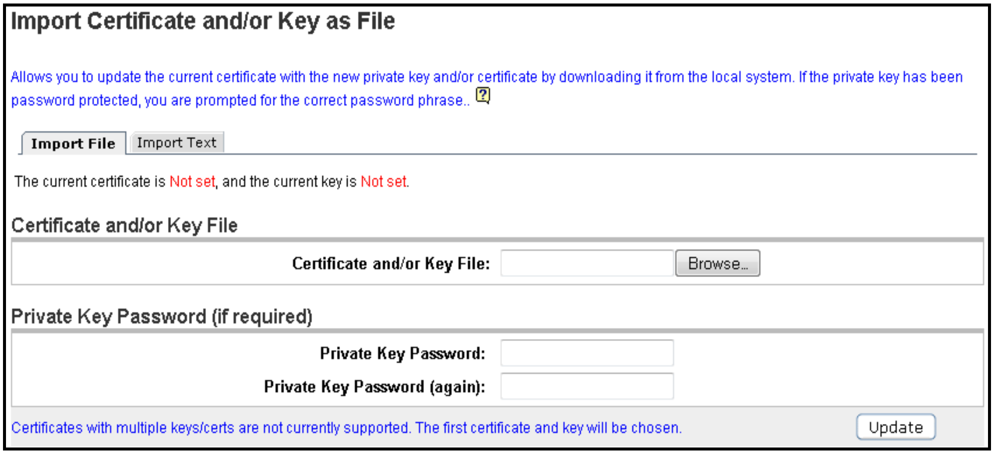
Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		
□	4		No	No	No		
□	5		No	No	No		
□	6	example server_cert	No	No	No		

5. **In Certificate Information form, in the name field select the certificate you wish to import to AVG.**

6. **In Certificate Summary form, under Settings select Import.**

   The Import Certificate as File form is displayed.



Import Certificate and/or Key as File

Allows you to update the current certificate with the new private key and/or certificate by downloading it from the local system. If the private key has been password protected, you are prompted for the correct password phrase..

The current certificate is Not set, and the current key is Not set.

Certificate and/or Key File

Certificate and/or Key File:

Private Key Password (if required)

Private Key Password:

Private Key Password (again):

Certificates with multiple keys/certs are not currently supported. The first certificate and key will be chosen.

7. **To import a certificate file, select Import File.**

   You can also paste the certificate you wish to import. In this case, select Import Text instead of Import File.

8. **Under Certificate and/or Key file, click Browse.**

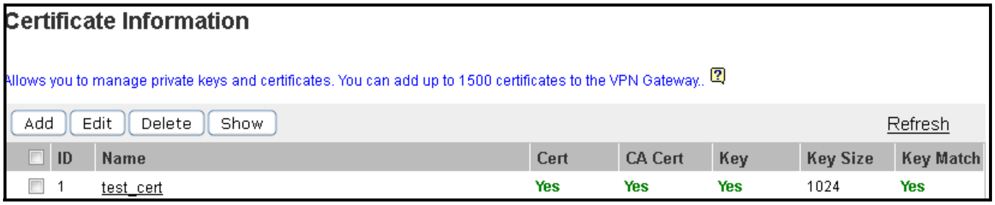
   The files in your file system are displayed.

9. **Double-click the certificate file you wish to import.**

10. **In the fields under Private Key Password, enter the import passphrase if required.**

11. **Click Update.**

12. **In the tree view, select Certificates to view the properties of the imported certificate.**



Certificate Information

Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

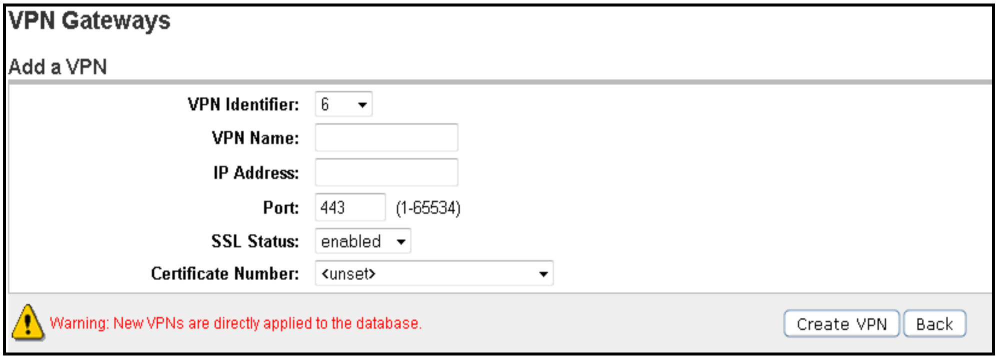
□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes

13. **Apply the changes.**

Configure the VPN

1. **In the System tree view, select VPN Gateways.**
2. **Click Add.**

   The Add VPN form is displayed.



VPN Gateways

Add a VPN

VPN Identifier:	6
VPN Name:	
IP Address:	
Port:	443 (1-65534)
SSL Status:	enabled
Certificate Number:	<unset>

Warning: New VPNs are directly applied to the database.

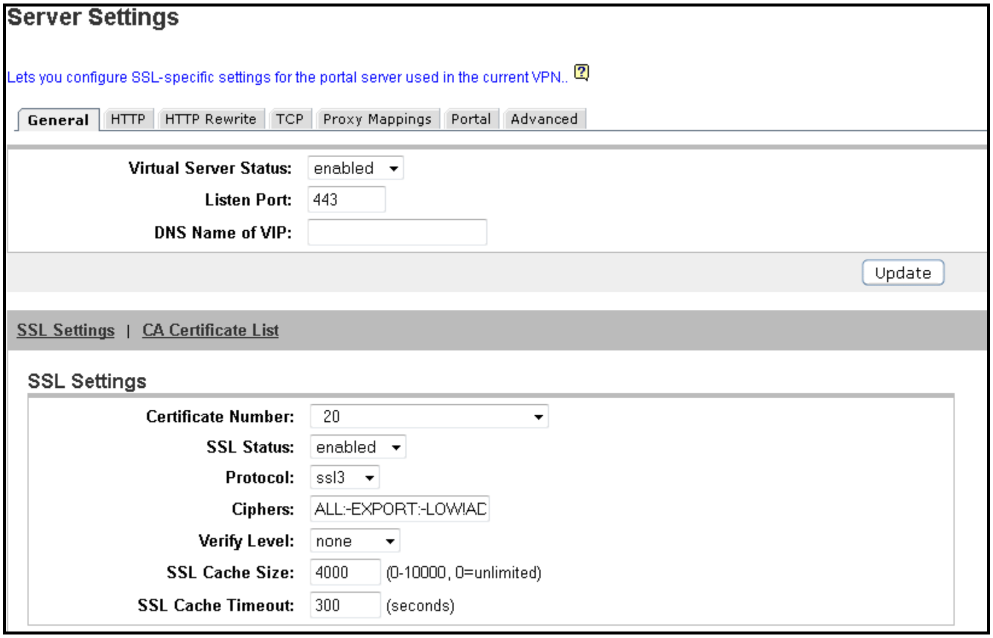
3. **In the System tree view, select VPN Gateways.**
4. **In the VPN Gateways form, in the Name field, select the name you want to enable standalone mode.**
5. **In VPN Summary form, select General.**

   The Session form is displayed.
6. **In the Standalone Status list box, select enabled and Click Update.**

   This step sets the portal server to standalone mode, which is required if the VPN Gateway is not connected to an application switch.
7. **In the System tree view, select VPN Gateways.**
8. **In the VPN Gateways form, in the Name field, select the name for which you want to enable standalone mode.**

   The VPN Summary form is displayed.
9. **Select SSL.**

The Server Settings form is displayed.



Server Settings

Lets you configure SSL-specific settings for the portal server used in the current VPN..

Virtual Server Status:	enabled
Listen Port:	443
DNS Name of VIP:	

SSL Settings

Certificate Number:	20
SSL Status:	enabled
Protocol:	ssl3
Ciphers:	ALL:-EXPORT:-LOW:!AD
Verify Level:	none
SSL Cache Size:	4000 (0-10000, 0=unlimited)
SSL Cache Timeout:	300 (seconds)

10. **Select General.**

11. **In the DNS Name of VIP field, enter a Fully Qualified Domain Name (FQDN) to the portal server.**

    The domain name you specify (in this example vpn.example1.com) should also be registered in DNS to resolve to the Portal IP address. The FQDN of the portal server corresponds to the URL that remote users will type in the address field of their web browser to access the Portal login page when the VPN is fully deployed.

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

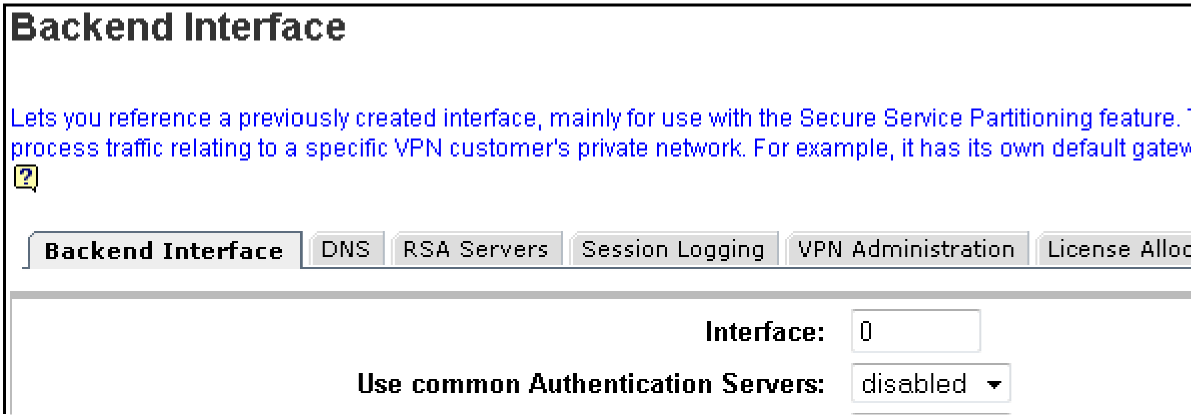
Bind VPN 1 to Interface 3 and Configure the DNS Settings

By binding VPN 1 to Interface 3, this interface will be the target for all private traffic for Company A.

1. **In the System tree view, select VPN Gateways.**
2. **Click on the VPN gateway name.**

   VPN Summary screen is displayed.
3. **Under Settings, select Advanced.**
4. **Click on Backend Interface tab.**

   Backend Interface screen appears.



Backend Interface

Lets you reference a previously created interface, mainly for use with the Secure Service Partitioning feature. T
process traffic relating to a specific VPN customer's private network. For example, it has its own default gatew

Interface: 0

Use common Authentication Servers: disabled

5. **In the Interface field, enter 3.**

   This binds VPN 1 to Interface 3.
6. **Configure the Avaya VPN Gateway to use common authentication servers (optional).**

   This step lets you enable common authentication for several VPNs, even if the VPNs are bound to specific interfaces. This ability can be used when the ISP wishes to share the same set of authentication servers for several end-customers.

   - `enabled`: Sets the Avaya VPN Gateway to use the default routing for authentication services.
   - `disabled`: Authentication requests will be routed through the referenced backend interface (see Step 5 above) to an authentication server on the end-customer’s private network.
7. **Configure the Avaya VPN Gateway to use common accounting servers (optional).**

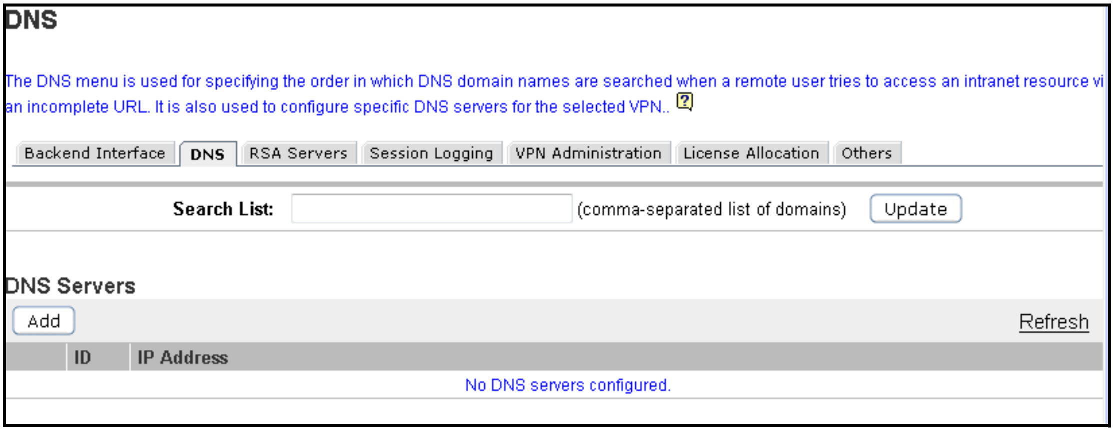
This step lets you enable common RADIUS accounting for several VPNs, even if the VPNs are bound to specific interfaces. This ability can be used when the ISP wishes to share the same set of accounting servers for several end-customers.

- `enabled`: Sets the Avaya VPN Gateway to use the default routing for accounting services.
- `disabled`: Accounting information will be routed through the referenced backend interface (see Step 5 above) to a RADIUS accounting server on the end-customer's private network.

8. **Click Update.**

9. **Click on the DNS tab.**

   The DNS form is displayed.



DNS

The DNS menu is used for specifying the order in which DNS domain names are searched when a remote user tries to access an intranet resource vi an incomplete URL. It is also used to configure specific DNS servers for the selected VPN..

Search List: (comma-separated list of domains)

DNS Servers

	ID	IP Address
No DNS servers configured.		

10. **In the Search List field, enter the desired search domains for the VPN.**

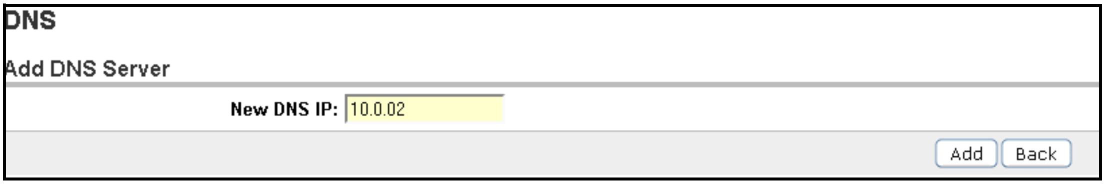
    The search domain(s) you specify are automatically appended to the host names a remote user types in the various address fields on the Portal (provided a match is found).

    Enter the search domains in a comma separated list, for example: `example1.com,support.example1.com`.

11. **Click Update.**

12. **Under DNS, click Add.**

    The DNS Settings form is displayed.



DNS

Add DNS Server

New DNS IP: 10.0.02

13. **In the New DNS IP field, configure the DNS server.**

    This step configures the system to use Company A's private DNS server. In this example, the IP address of Company A's DNS server is `10.0.0.2`.

14. **Click Add.**

15. **Apply the changes.**

Create IP Pool

The IP Pool comes into play when the remote user tries to access a host using Net Direct or the Avaya VPN Client. A new IP address has to be assigned as source IP for the unencrypted connection between the Avaya VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

As the ISP administrator, you can configure several IP Pools, each with a unique ID number and unique properties. By mapping the desired IP Pool to a user group, the end-customer can then establish 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 for the VPN. Groups for which no IP Pool is assigned (IP Pool number=0) will use the default IP Pool.

For more information about the Net Direct client and the Avaya VPN Client, see Chapter 7, "Net Direct" and Chapter 21, "Transparent Mode", respectively.

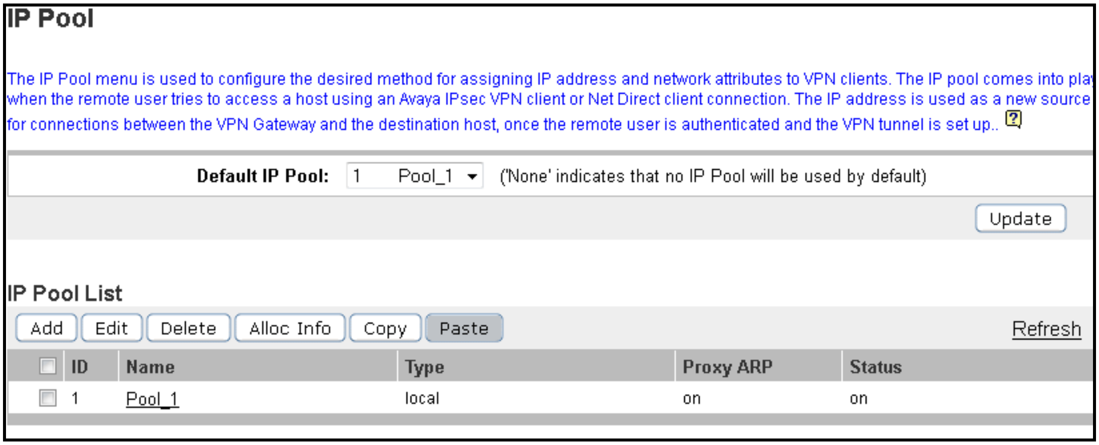
1. **In the System tree view, select VPN Gateways. The VPN Gateways form is displayed.**

2. **In the Name field, select the name for which you want to create IP Pool.**

    The VPN Summary form is displayed.

3. **Under Settings, select IP Pool.**

The IP Pool form is displayed.



IP Pool

The IP Pool menu is used to configure the desired method for assigning IP address and network attributes to VPN clients. The IP pool comes into pla when the remote user tries to access a host using an Avaya IPsec VPN client or Net Direct client connection. The IP address is used as a new source for connections between the VPN Gateway and the destination host, once the remote user is authenticated and the VPN tunnel is set up..

Default IP Pool: 1 Pool_1 ('None' indicates that no IP Pool will be used by default)

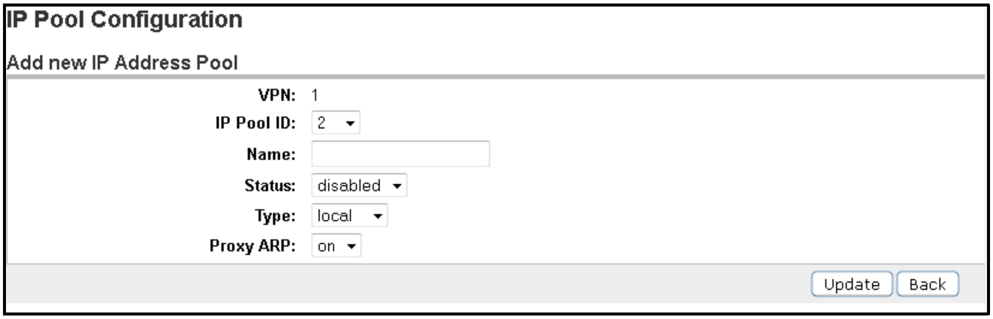
Update

IP Pool List

□	ID	Name	Type	Proxy ARP	Status
□	1	Pool_1	local	on	on

4. **Under IP Pool List, click Add.**

   The IP Pool Configuration form is displayed.



IP Pool Configuration

Add new IP Address Pool

VPN:	1
IP Pool ID:	2
Name:	
Status:	disabled
Type:	local
Proxy ARP:	on

   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 (from the Avaya VPN Gateway), from an external RADIUS server or from an external DHCP server.

   For IP Pools of the `local` type, network attributes should be configured on the Avaya VPN Gateway (see next section). For IP Pools of the `radius` and `dhcp` types, network attributes can be configured on the Avaya VPN Gateway 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 Avaya 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 Avaya 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.**

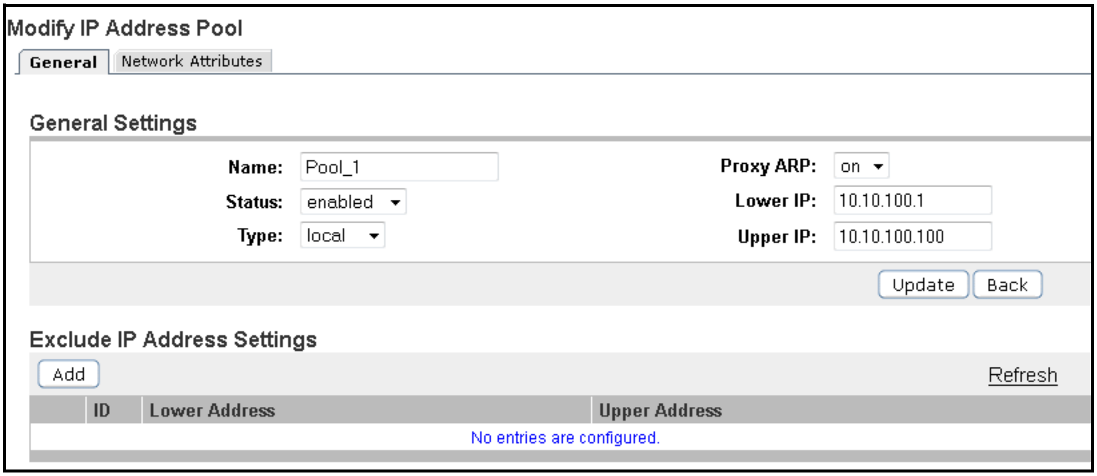
   Depending on which pool mechanism (`local`, `radius` or `dhcp`) you have selected, the IP Pool Configuration form now displays different input fields. Follow the relevant following description depending on your choice.

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism t to `local` (as described in Step 7 in the previous section), you should configure the desired IP address range. You can also configure network attributes to be retrieved from the Avaya VPN Gateway 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. **Enter the General Settings in IP Pool Configuration form.**



Modify IP Address Pool

General Settings

Name:	Pool_1	Proxy ARP:	on
Status:	enabled	Lower IP:	10.10.100.1
Type:	local	Upper IP:	10.10.100.100

Exclude IP Address Settings

	ID	Lower Address	Upper Address
No entries are configured.			

2. **Select Network Attributes Settings tab and configure the desired network attributes settings (optional).**

The Net Direct and Avaya VPN Client normally work 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 Step 1. 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** >>**VPN #** >> **Advanced** >> **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 or Avaya VPN Client 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 pool mechanism to `radius` (as described in the section "Create IP Pool" on page 517), you should configure the Avaya VPN Gateway to retrieve network attributes from a RADIUS server.

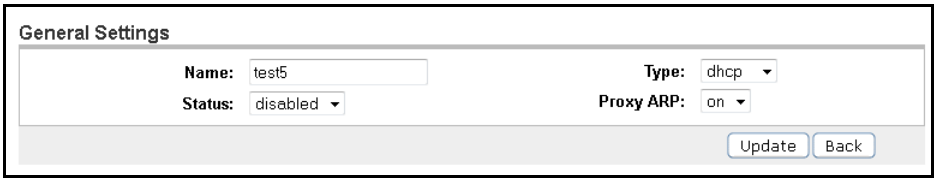
How to configure a RADIUS server is described in Chapter 9, "Authentication Methods".

To configure the Avaya VPN Gateway to retrieve network settings (including client IP address) through RADIUS attributes from an external RADIUS server, go to **VPN Gateways >> VPN # >> Authentication >> Radius >> Network Attributes.** A minimum requirement is to configure retrieval of client IP address and primary DNS server. You can retrieve a number of network attributes, e.g. primary/secondary DNS server, primary/secondary NBNS server and so on.

Network attributes can also be configured on the Avaya VPN Gateway 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 520 for instructions).

Configure DHCP Network Attributes

If you set the pool mechanism to `dhcp` (as described in the section "Create IP Pool" on page 517), you should configure the Avaya VPN Gateway to retrieve network attributes from a DHCP server.



General Settings

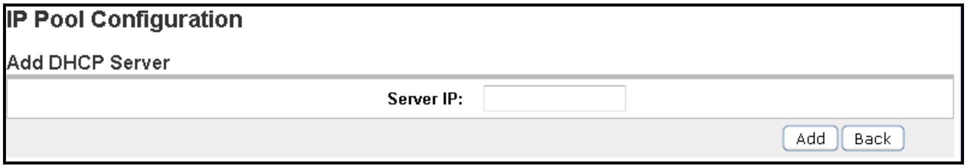
Name: test5

Type: dhcp

Status: disabled

Proxy ARP: on

1. **Under DHCP Servers, click Add.**
2. **Configure the external DHCP server IP address.**



IP Pool Configuration

Add DHCP Server

Server IP:

3. **Click Add.**
4. **Apply the changes.**

Network attributes can also be configured on the Avaya VPN Gateway 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 520 for instructions).

Create Default IP Pool

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

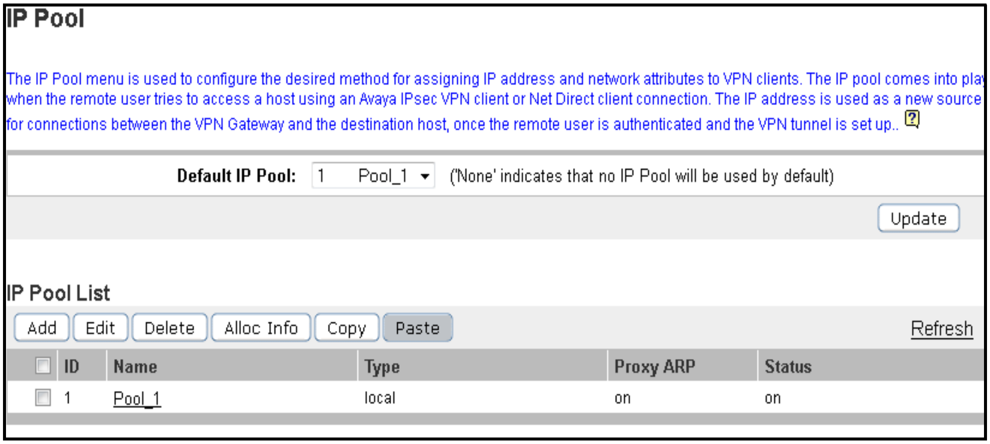
1. **In the System tree view, select VPN Gateways. The VPN Gateways form is displayed.**

2. **In the Name field, select the name for which you want to create default IP Pool.**

   The VPN Summary form is displayed.

3. **Under Settings, select IP Pool.**

   The IP Pool form is displayed.



IP Pool

The IP Pool menu is used to configure the desired method for assigning IP address and network attributes to VPN clients. The IP pool comes into play when the remote user tries to access a host using an Avaya IPsec VPN client or Net Direct client connection. The IP address is used as a new source for connections between the VPN Gateway and the destination host, once the remote user is authenticated and the VPN tunnel is set up..

Default IP Pool: 1 Pool_1 ('None' indicates that no IP Pool will be used by default)

IP Pool List

☐	ID	Name	Type	Proxy ARP	Status
☐	1	Pool_1	local	on	on

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)

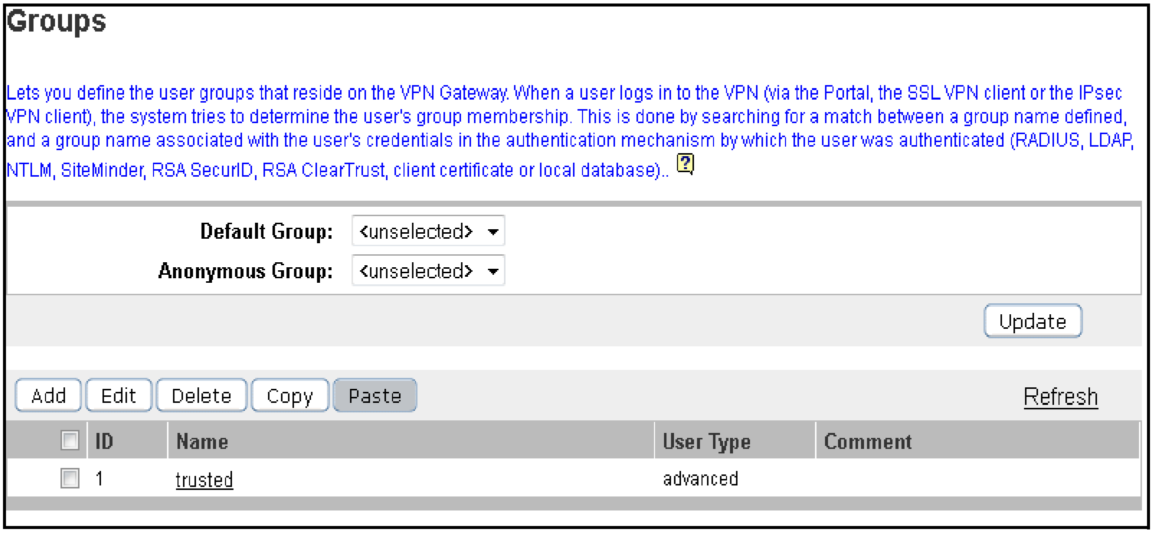
As mentioned in the section "Create IP Pool" on page 517, several IP Pools with different mechanisms (that is, `local`, `radius` or `dhcp`) can be configured. By mapping the IP Pools to different user groups you can provide different ways of assigning IP address and network attributes depending on the user's group membership.

One of the configured IP Pools should be selected as the default IP Pool for the VPN. 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. The VPN Gateways form is displayed.**
2. **In the Name field, select the name for which you want to map an IP Pool.**

   The VPN Summary form is displayed.
3. **Under Settings, select Groups.**
4. **Select the check box next to group to which you want to map an IP Pool.**
5. **Select the check box next to the group to which you want to map an IP Pool.**



Groups

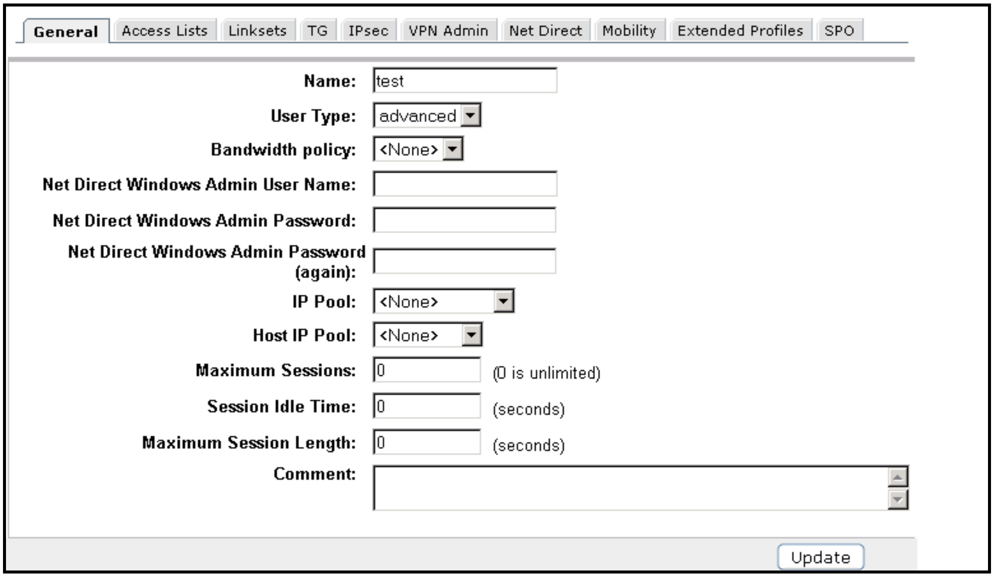
Lets you define the user groups that reside on the VPN Gateway. When a user logs in to the VPN (via the Portal, the SSL VPN client or the IPsec VPN client), the system tries to determine the user's group membership. This is done by searching for a match between a group name defined, and a group name associated with the user's credentials in the authentication mechanism by which the user was authenticated (RADIUS, LDAP, NTLM, SiteMinder, RSA SecurID, RSA ClearTrust, client certificate or local database).. ?

Default Group:	<unselected>
Anonymous Group:	<unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

6. **Click Edit.**

7. **In the IP Pool list box, select the IP Pool that you wish to map to the current group.**



Name:	test
User Type:	advanced
Bandwidth policy:	<None>
Net Direct Windows Admin User Name:	
Net Direct Windows Admin Password:	
Net Direct Windows Admin Password (again):	
IP Pool:	<None>
Host IP Pool:	<None>
Maximum Sessions:	0 (0 is unlimited)
Session Idle Time:	0 (seconds)
Maximum Session Length:	0 (seconds)
Comment:	

8. **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.

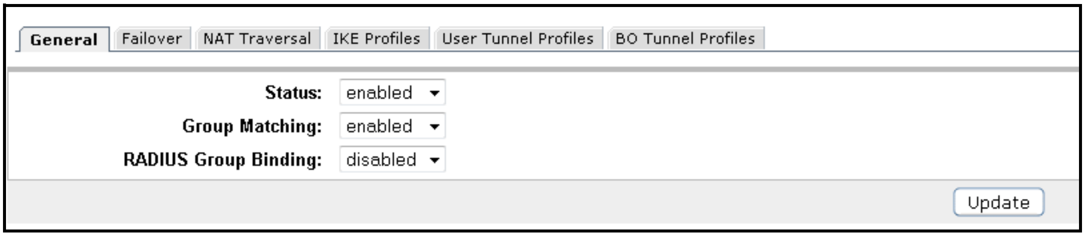
Enable IPsec

To enable access to the VPN through IPsec *user tunnels* (that is, for remote users with the Avaya VPN Client installed using IPSec) or IPsec *branch office* tunnels, proceed as follows:

1. **In the System tree view, select VPN Gateways. The VPN Gateways form is displayed.**
2. **In the Name field, select the name for which you want to enable IPsec.**

   The VPN Summary form is displayed.
3. **Under Settings, select IPsec.**

The IPsec General form is displayed.



Status: enabled

Group Matching: enabled

RADIUS Group Binding: disabled

4. **In the Status list box, select `enabled`.**
5. **Click Update and apply the changes.**

IPsec User Tunnel Configuration

Once IPsec has been enabled for the VPN, the end-customer can configure the IPsec user tunnel(s) through the VPN Administrator web user interface. If the end-customer wishes to use local client IP address assignment instead of retrieving network attributes (including client IP address) from a RADIUS server, the IP Pool must also be configured before the end-customer can continue with the configuration.

IPsec user tunnel configuration is described in the section "Configuring Avaya VPN Client (IPsec)" on page 604 in Chapter 21, "Transparent Mode" in this Application Guide and in the same section in the "Transparent Mode" chapter in the *VPN Administrator's Guide*.

IPsec Branch Office Tunnel Configuration

Once IPsec has been enabled for the VPN, the end-customer can configure the IPsec branch office tunnel(s) through the VPN Administrator web user interface.

IPsec branch office tunnel configuration is described in Chapter 18, "Branch Office Tunnels" in this Application Guide and in the "Branch Office Tunnels" chapter in the *VPN Administrator's Guide*.

License Allocation

By default, the SSL and IPsec user licenses you may have loaded to the Avaya VPN Gateway cluster are shared by all VPNs. Using the license allocation feature, you can however dedicate a certain number of concurrent users to different VPNs. For example, an SSL user license valid for 2000 concurrent users can be distributed as desired amongst configured VPNs. Also see "License Pool (SSL and IPsec Users)" on page 76 in Chapter 4, "VPN Introduction".

1. **In the System tree view, select VPN Gateways.**

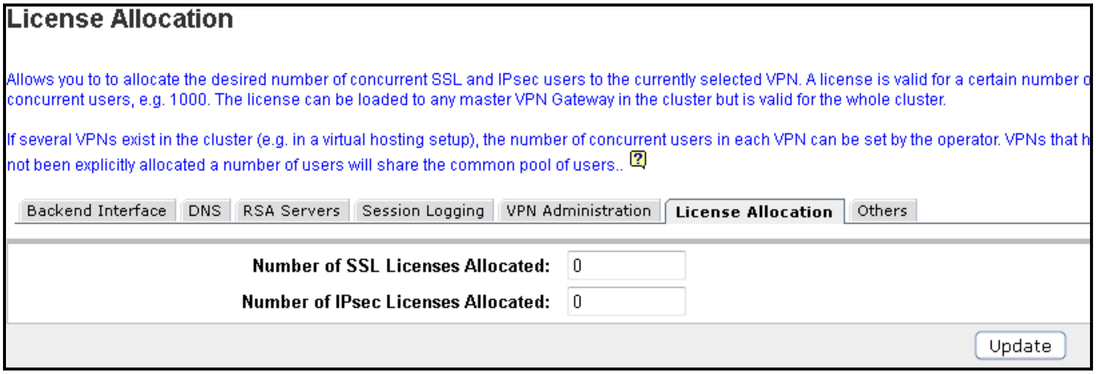
2. **Click on the name of the VPN Gateway.**

   VPN Summary screen appears.

3. **Under Settings, select Advanced.**

4. **Click on License Allocation tab.**

   The License Allocation form is displayed.



License Allocation

Allows you to to allocate the desired number of concurrent SSL and IPsec users to the currently selected VPN. A license is valid for a certain number o concurrent users, e.g. 1000. The license can be loaded to any master VPN Gateway in the cluster but is valid for the whole cluster.

If several VPNs exist in the cluster (e.g. in a virtual hosting setup), the number of concurrent users in each VPN can be set by the operator. VPNs that h not been explicitly allocated a number of users will share the common pool of users..

Number of SSL Licenses Allocated: 0

Number of IPsec Licenses Allocated: 0

5. **In the Number of SSL Licenses Allocated field, enter the desired number of concurrent SSL users to VPN 1.**

6. **In the Number of IPsec Licenses Allocated field, enter the desired number of concurrent IPsec users to VPN 1.**

7. **Click Update and apply your changes.**

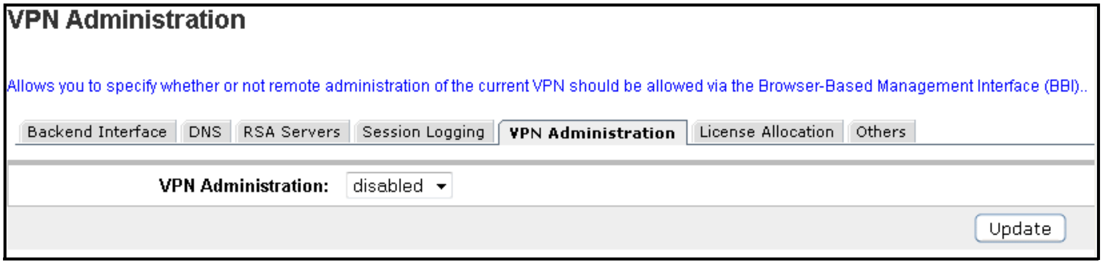
VPN Administration

When VPN administration is enabled, end-customers can themselves manage certain configuration options for their VPNs through a web user interface. To access the web user interface, navigate through the path **VPN Gateway >> VPN #>> Advanced >> VPN Administration**.

1. **In the System tree view, select VPN Gateways.**
2. **Click on the VPN Gateway name.**

   VPN Summary screen appears.
3. **Under Settings, select Advanced.**
4. **Select VPN Administration.**

   The VPN Administration form is displayed.



VPN Administration

Allows you to specify whether or not remote administration of the current VPN should be allowed via the Browser-Based Management Interface (BBI)..

VPN Administration: disabled

5. **In the VPN Administration list box, select `enabled`.**

   This enables VPN administration globally for the VPN.
6. **Click Update.**

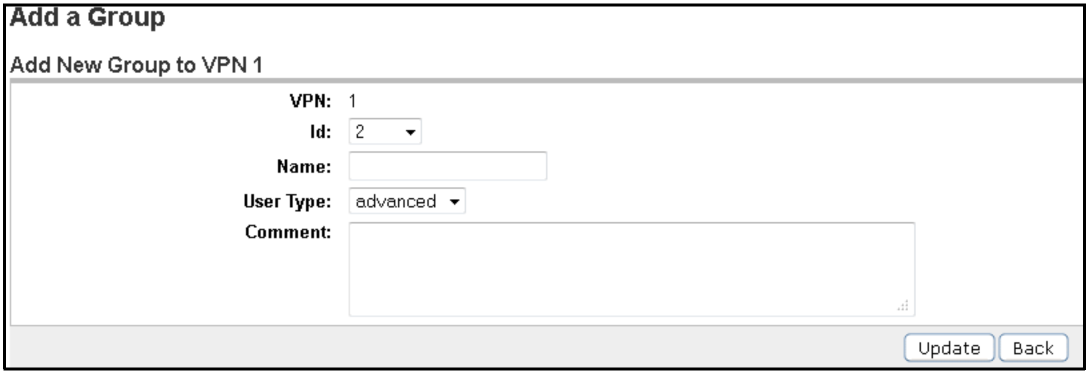
Configure VPN Administrator Access Group

The next step is to enable VPN administration for the desired user access group.

1. **In the System tree view, select VPN Gateways.**
2. **Click on the VPN Gateway name.**

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

The Add New Group form is displayed.



Add a Group

Add New Group to VPN 1

VPN: 1

Id: 2

Name:

User Type: advanced

Comment:

5. **In the Name field, enter a name for the group, for example `vpn_admin`.**

6. **Click Update.**

7. **In the System tree view, select VPN Gateways.**

8. **Click on the VPN Gateway name.**

   VPN Summary screen appears.

9. **Under Settings, select Advanced.**

10. **Click on VPN Administration tab.**

    The VPN Admin form is appears.

11. **In the Group list box, select the group for which you wish to enable VPN administration (if not already displayed) and click Refresh.**

12. **In the VPN Administration list box, select `enabled`.**

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

Configure Access Rules for the VPN Administrator Group

1. **In the System tree view, under Groups, select Access List.**

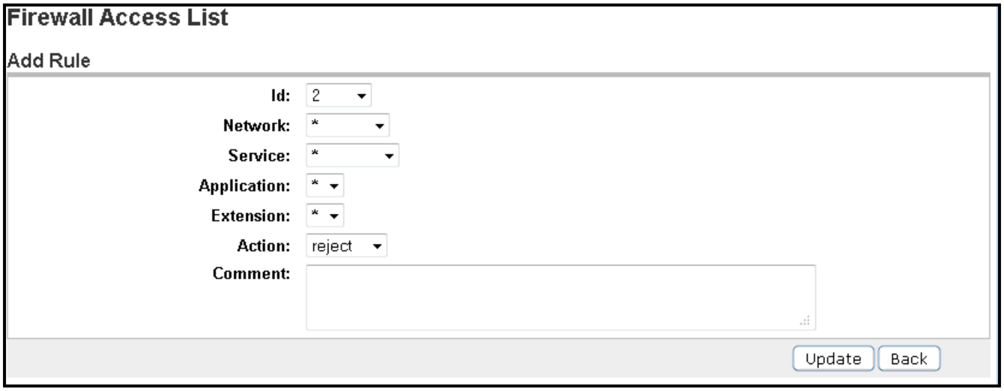
   The Firewall Access List form is displayed.

2. **In the VPN Number and Group list boxes respectively, select the desired VPN and the Group for which you want to configure access rules.**

   If you have created a group called vpn_admin (like in the example on the previous page), select this name in the Group list box.

3. **Click Add.**

   The Add Rule form is displayed.



Firewall Access List

Add Rule

Id: 2

Network: *

Service: *

Application: *

Extension: *

Action: reject

Comment:

4. **Leave the asterisks (*) in the Network, Service and Application list boxes. This implies that access to all networks, protocols and paths is allowed.**

5. **In the Action list box, select `accept`.**

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

NOTE – The VPN Administrator group configured in the preceding example has full access to all networks and services. If you wish to configure less generous access rights (for example to limit access to a specific network), you should first configure the desired network definition(s) so they can be selected in the Network list box in the Firewall Access list form. For instructions, see Chapter 8, "Groups, Access Rules and Profiles".

Configure VPN Administrator User

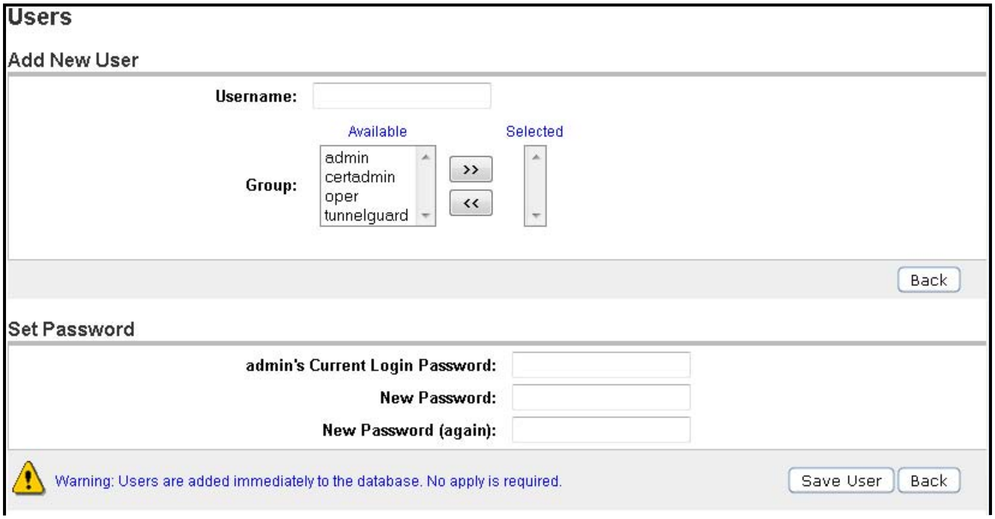
The following steps show how to configure a user in the Avaya VPN Gateway’s local database and map this user to the VPN Administrator group configured in the previous example. This instruction assumes that you have already configured a local database. If not, see the section “Local Database Authentication” on page 240 in Chapter 9, “Authentication Methods”.

1. **In the System tree view, expand Administration.**

2. **Select Users.**

3. **Under Users, click Add.**

   The Add Single User form is displayed.



Warning: Users are added immediately to the database. No apply is required.

4. **In the Name field, enter the user’s user name.**

5. **In the Password fields, enter the user’s password.**

6. **Move the `vpn_admin` group to the Selected list.**

   This action makes the user a member of the `vpn_admin` group.

7. **Click Save User.**

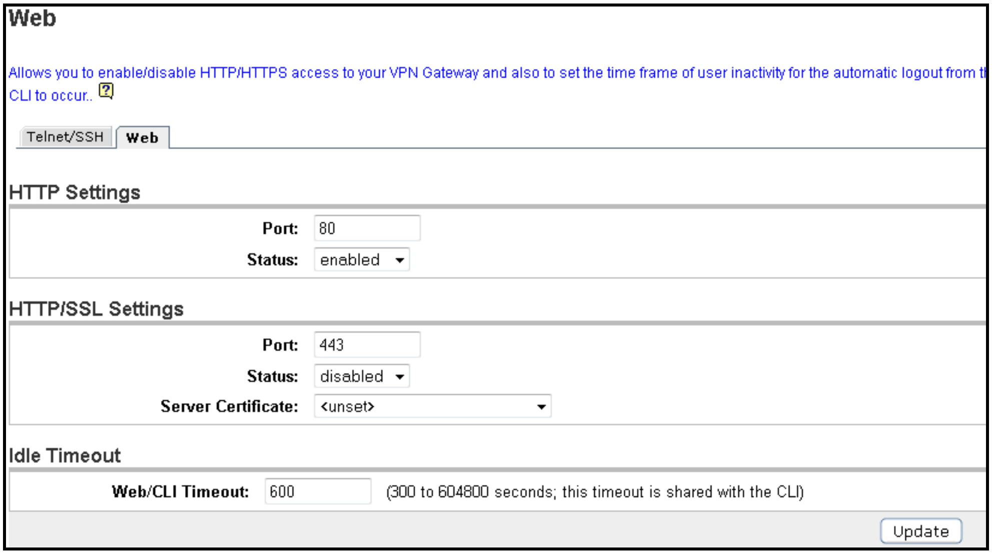
Enable Access to Web Interface through HTTP or HTTPS

For VPN Administrators to be able to access the web user interface, access through HTTP or HTTPS should be enabled. If you are currently configuring the system through the BBI, this has already been done. The setting is global for the cluster, that is, all VPN administrators will have access to their VPNs once access is enabled.

You may however want to change or add a protocol, for example HTTPS, if you have previously only enabled access through HTTP.

1. **In the System tree view, expand Administration and select Remote Access, Web.**

   The Web Settings form is displayed.



Web

Allows you to enable/disable HTTP/HTTPS access to your VPN Gateway and also to set the time frame of user inactivity for the automatic logout from t
CLI to occur..

HTTP Settings

Port: 80
Status: enabled

HTTP/SSL Settings

Port: 443
Status: disabled
Server Certificate: <unset>

Idle Timeout

Web/CLI Timeout: 600 (300 to 604800 seconds; this timeout is shared with the CLI)

2. **Select the desired port and enable access to the Avaya VPN Gateway cluster through HTTP or HTTPS.**

3. **Click Update.**

4. **Apply the changes.**

   Users that are members of an access group where VPN administration is allowed can now manage the settings for their VPN through the web user interface.

Configure VPN 2

To configure VPN 2, simply follow the steps in the section “Configure VPN 1” on page 510 but substitute the values with values that are appropriate for VPN 2.

Update DNS Server

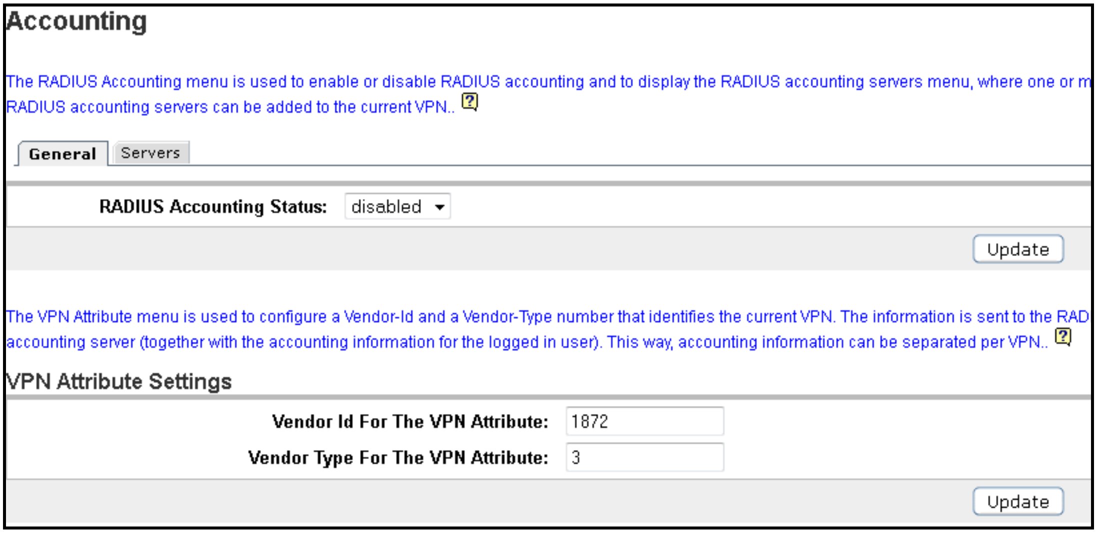
The local DNS servers should be updated with the domain names used for the VPNs, and be configured to perform reverse DNS lookups.

Configure RADIUS accounting server

This section explains how to configure the RADIUS accounting servers.

1. **In the System tree view, select VPN Gateways.**
2. **Click on the VPN Gateway name.**

   VPN Summary screen appears.
3. **Under Settings, select Accounting.**
4. **Click General tab.**



Accounting

The RADIUS Accounting menu is used to enable or disable RADIUS accounting and to display the RADIUS accounting servers menu, where one or m RADIUS accounting servers can be added to the current VPN..

RADIUS Accounting Status: disabled

The VPN Attribute menu is used to configure a Vendor-Id and a Vendor-Type number that identifies the current VPN. The information is sent to the RAD accounting server (together with the accounting information for the logged in user). This way, accounting information can be separated per VPN..

VPN Attribute Settings

Vendor Id For The VPN Attribute: 1872

Vendor Type For The VPN Attribute: 3

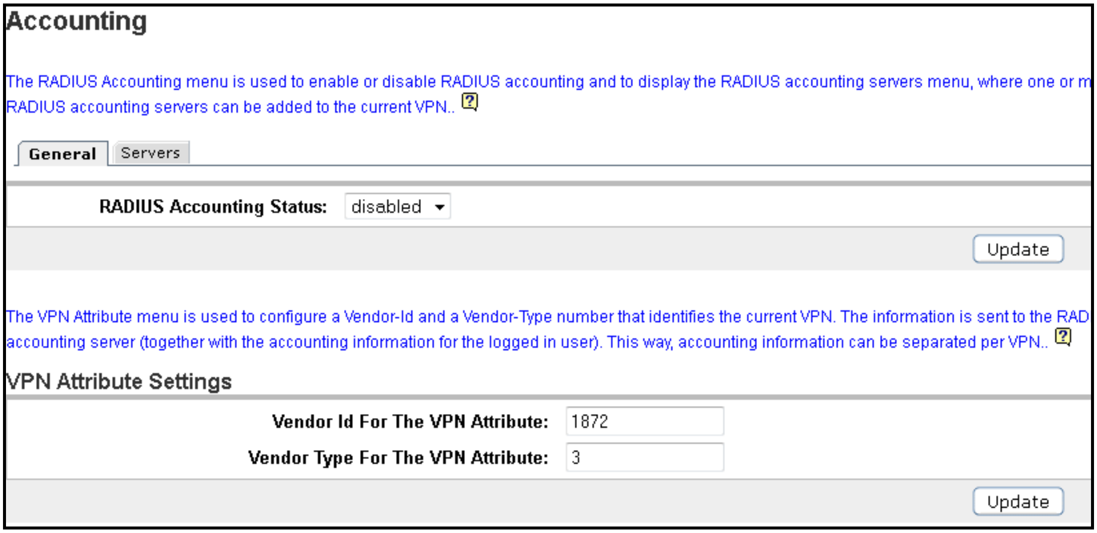
5. **Set RADIUS Accounting Status enabled.**
6. **Click Update.**

Configure Vendor-Id and Vendor-Type

The VPN Attribute section is used to configure a Vendor-Id and a Vendor-Type number that identifies the current VPN domain. The information is sent to the RADIUS accounting server (together with the accounting information for the logged in user). This way, accounting information can be separated per VPN domain.

1. **In the System tree view, select VPN Gateways.**
2. **Click on the VPN Gateway name.**

   VPN Summary screen appears.
3. **Under Settings, select Accounting.**
4. **Click General tab.**



Accounting

The RADIUS Accounting menu is used to enable or disable RADIUS accounting and to display the RADIUS accounting servers menu, where one or m
RADIUS accounting servers can be added to the current VPN..

RADIUS Accounting Status: disabled

The VPN Attribute menu is used to configure a Vendor-Id and a Vendor-Type number that identifies the current VPN. The information is sent to the RAD
accounting server (together with the accounting information for the logged in user). This way, accounting information can be separated per VPN..

VPN Attribute Settings

Vendor Id For The VPN Attribute: 1872

Vendor Type For The VPN Attribute: 3

5. **Assign the SMI Network Management Private Enterprise Code -- as defined by IANA in the file http://www.iana.org/assignments/enterprise-numbers -- to the Vendor-Id attribute.**

   The Vendor-Id -- represented by the private enterprise number -- is one of the RADIUS vendor-specific attributes.

   The default Vendor Id is 1872 (Alteon).
6. **Assigns a number to the Vendor-Type attribute used in RADIUS. Used in combination with the Vendor-Id number, the Vendor-Type number identifies the attribute which will contain the accounting information.**

The default Vendor Type value is 3.

7. **Click Update.**

Adding RADIUS Accounting Server

Allows the user to add one or more RADIUS accounting servers to the current configuration. With a RADIUS accounting server configured, an accounting request start packet will automatically be sent to the accounting server for each user who successfully authenticates to the Avaya VPN Gateway. The start packet contains the following information:

- Client user name
- Avaya VPN Gateway IP address
- Session id

When a user session is terminated, an accounting request stop packet is sent to the accounting server containing the following information:

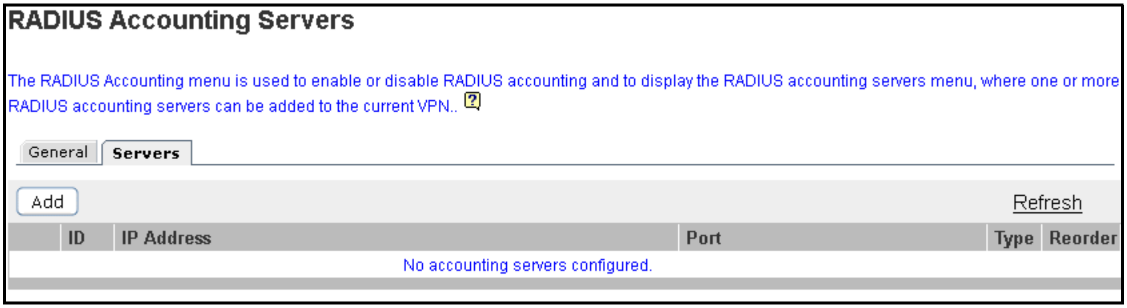
- Session id
- Session time
- Cause of termination

Follow these steps to add a RADIUS accounting server.

1. **In the System tree view, select VPN Gateways.**
2. **Click on the VPN Gateway name.**

   VPN Summary screen appears.
3. **Under Settings, select Accounting.**
4. **Click ServerSpecify whether the accounting server is SSP-specific or System-wide. tab.**

RADIUS Accounting Servers form is displayed.

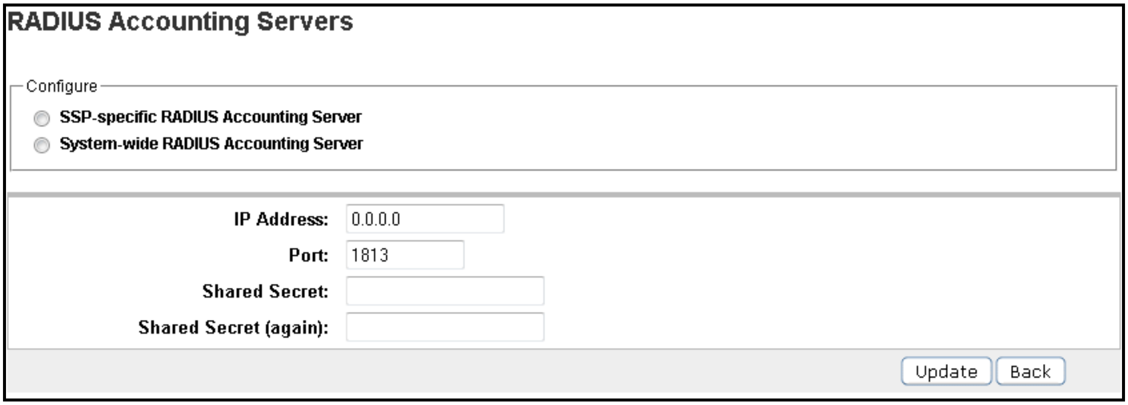


RADIUS Accounting Servers

The RADIUS Accounting menu is used to enable or disable RADIUS accounting and to display the RADIUS accounting servers menu, where one or more RADIUS accounting servers can be added to the current VPN..

	ID	IP Address	Port	Type	Reorder
No accounting servers configured.					

5. **Click Add.**



RADIUS Accounting Servers

Configure

○ SSP-specific RADIUS Accounting Server

○ System-wide RADIUS Accounting Server

IP Address: 0.0.0.0

Port: 1813

Shared Secret:

Shared Secret (again):

6. **Specify whether the accounting server is SSP-specific or System-wide.**

7. **Specify the IP address of the RADIUS accounting server.**

   For backup purposes, several RADIUS accounting servers can be added. The Avaya VPN Gateway will contact the server with the lowest index number first. If contact cannot be established, the Avaya VPN Gateway will try to contact the server with the next index number in sequence, and so on.

   NOTE – Note: The default port number used for RADIUS accounting is 1813.

8. **Specify the TCP port number.**

9. **Specify the RADIUS shared secret.**

10. **Click Update.**

Remaining Configuration

Once you have configured the basics for a VPN, you can delegate per domain configuration to members of the VPN Admin group within the VPN. This allows the end-customer in a managed VPN service to configure authentication methods, user access groups, access rules, linksets, Avaya Endpoint Access Control Agent checks, WholeSecurity scans and much more.

The end-customers can also customize their Portals, for example change the color theme, banner and static texts. Note that the total size of imported banners in the different VPNs in the cluster must not exceed 16 MB.

End-user instructions on how to manage their own VPNs through the web user interface are provided in the *VPN Administrator's Guide*.

CHAPTER 18

Branch Office Tunnels

In addition to IPsec-based *user* tunnels, where the remote user connects to the Avaya VPN Gateway through an IPsec VPN client, the Avaya VPN Gateway 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 Avaya VPN Gateway. When there are more than one Avaya 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 Avaya VPN Gateways on the public side of the cluster.

User clients, such as the Avaya VPN Client, 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 Avaya VPN Gateways in the cluster. The branch office tunnel will be established from the Avaya VPN Gateway that currently owns the Portal IP address.

If a cluster member (Avaya VPN Gateway) 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 Avaya VPN Gateway(s).

Scalability and Load Balancing

To achieve higher capacity, more Avaya VPN Gateways can be added to the cluster. If there are two Avaya VPN Gateways 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 Avaya VPN Gateway to the cluster.

Connection Example

Refer to Figure 18-1 on page 542.

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 Avaya VPN Gateway.

2. The Avaya 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 Avaya 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 Avaya 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 “Configuration Example” on page 543).

5. The Avaya 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 Avaya 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 Avaya 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 Avaya VPN Gateway should be mirrored in the BO configuration on the BO’s Avaya 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 above steps are exactly the same, only reversed.

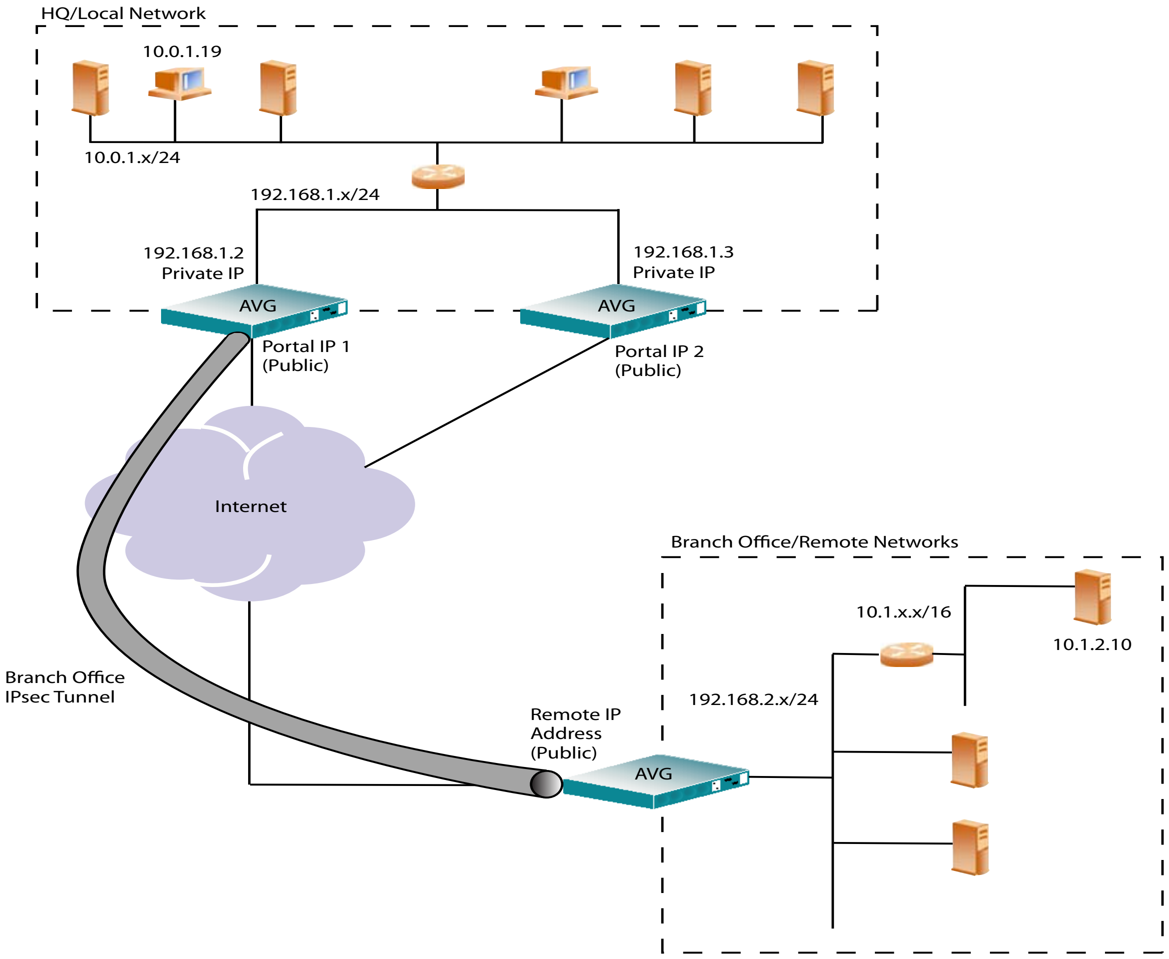


Figure 18-1 Branch Office Tunnel

The above configuration shows two Avaya VPN Gateways in a cluster. If the Avaya VPN Gateway that currently owns the BO tunnel fails, the tunnel migrates to the other Avaya VPN Gateway. For the networks on the private side to be aware of the tunnel shift and thus send the packets to the right AVG, the Avaya VPN Gateway 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.

Initial Setup

Before you can start configuring the branch office tunnel you should perform an initial setup of the system. The initial setup procedure is described in the “Initial Setup” chapter in the *User’s Guide*.

Basic VPN Setup

If the VPN Gateway should be used to configure a basic VPN, see Chapter 5, “Clientless Mode”.

Secure Service Partitioning

If the Avaya VPN Gateway should be used to perform secure service partitioning, that is, host VPNs for different end-customers, go to Chapter 17, “Secure Service Partitioning” for instructions on how to configure interfaces for the different VPNs, configure the VPNs and bind the interfaces to the VPNs.

Configure Branch Office Tunnel

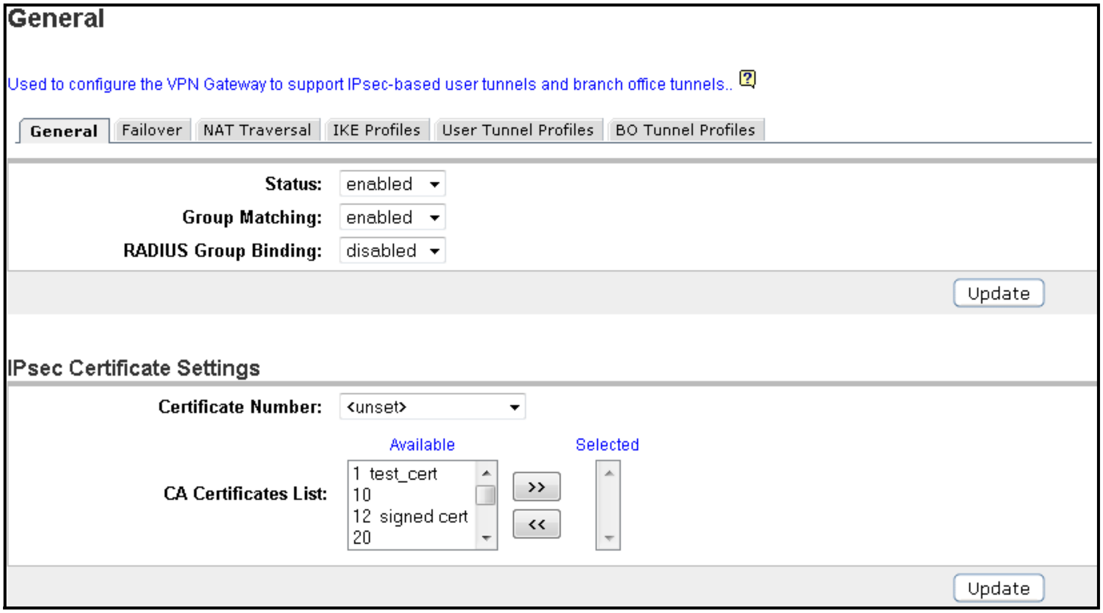
Branch office tunnels use IPsec for secure transfer of packets. To enable to the IKE daemon (IPsec server) on the Avaya VPN Gateway, proceed as follows:

Enable IPsec

1. **Log on to the BBI as administrator user.**
2. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form is displayed.
3. **Select the configured VPN for which you want to enable IPsec.**

   The VPN Summary form is displayed.
4. **Under Settings, select IP Sec. The General form is displayed.**
5. **Click General.**



General

Used to configure the VPN Gateway to support IPsec-based user tunnels and branch office tunnels..

Status: enabled

Group Matching: enabled

RADIUS Group Binding: disabled

IPsec Certificate Settings

Certificate Number: <unset>

CA Certificates List:

Available: 1 test_cert, 10, 12 signed cert, 20

Selected:

6. **In the Status list box, select enabled.**
7. **Specify whether to enable or disable the group match for the group authentication option. The default value is enabled, which matches the groups returned for the user**

authentication. When disabled, user will be placed on the group that is used for the group session.

8. **Click Update.**

IPSec Failover

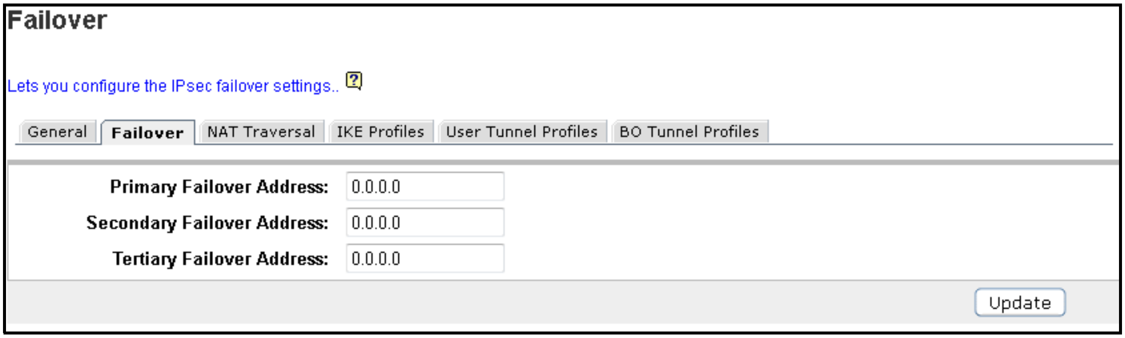
1. **Log on to the BBI as administrator user.**
2. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form is displayed.

3. **Select the configured VPN for which you want to enable IPsec.**

   The VPN Summary form is displayed.

4. **Under Settings, select IP Sec.**
5. **Click Failover.**



Primary Failover Address: 0.0.0.0
Secondary Failover Address: 0.0.0.0
Tertiary Failover Address: 0.0.0.0

6. **Specify the primary, secondary, and tertiary IP address for IPsec failover.**
7. **Click Update.**
8. **Click Apply to apply the changes.**

NAT Traversal

This procedure lets you configure the IPsec NAT traversal settings.

1. **Log on to the BBI as administrator user.**
2. **In the System tree view, select VPN Gateways.**

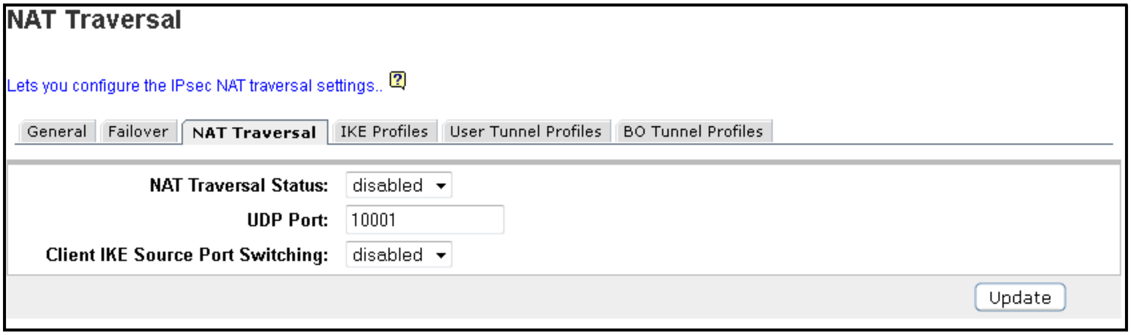
   The VPN Gateways form is displayed.

3. **Select the configured VPN for which you want to enable IPsec.**

   The VPN Summary form is displayed.

4. **Under Settings, select IP Sec.**

5. **Click NAT Traversal.**



NAT Traversal

Lets you configure the IPsec NAT traversal settings..

NAT Traversal Status: disabled

UDP Port: 10001

Client IKE Source Port Switching: disabled

6. **Enable the status of the NAT traversal.**

7. **Specify the UDP port number.**

   The UDP port number should be an integer value.

8. **Enable Client IKE source port switching.**

9. **Click update to update the specified settings for the pending configuration.**

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 Avaya VPN Gateway.

For instructions on how to create access groups, see Chapter 8, “Groups, Access Rules and Profiles”.

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 *User's Guide*.

In a secure service partitioning configuration, the IKE profile can also be configured by the end-customer (with VPN administration rights) through the web user interface.

1. **Log on to the BBI as administrator user.**
2. **In the System tree view, select VPN Gateways.**

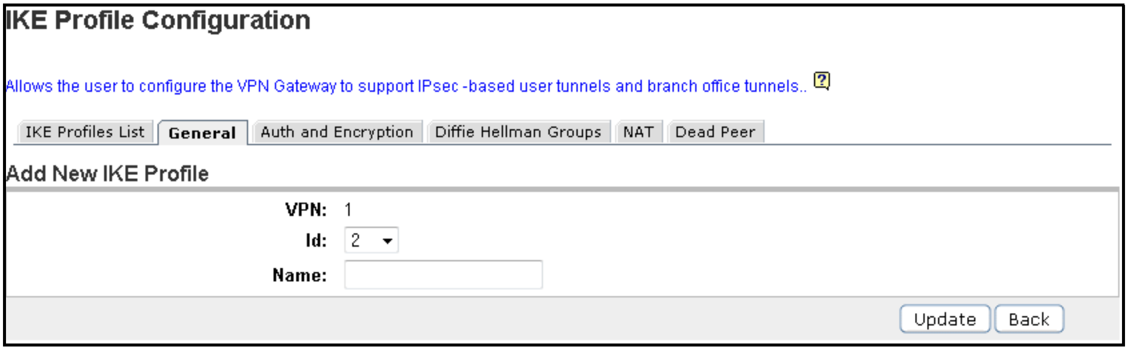
   The VPN Gateways form is displayed.
3. **Select the configured VPN for which you to create an IKE profile.**

   The VPN Summary form is displayed.
4. **Under Settings, select IP Sec.**

   The General form is displayed.
5. **Select IKE Profiles.**

   The IKE Profiles form is displayed.
6. **Click Add.**

   The Add New IKE Profile form is displayed.



IKE Profile Configuration

Allows the user to configure the VPN Gateway to support IPsec -based user tunnels and branch office tunnels..

Add New IKE Profile

VPN: 1

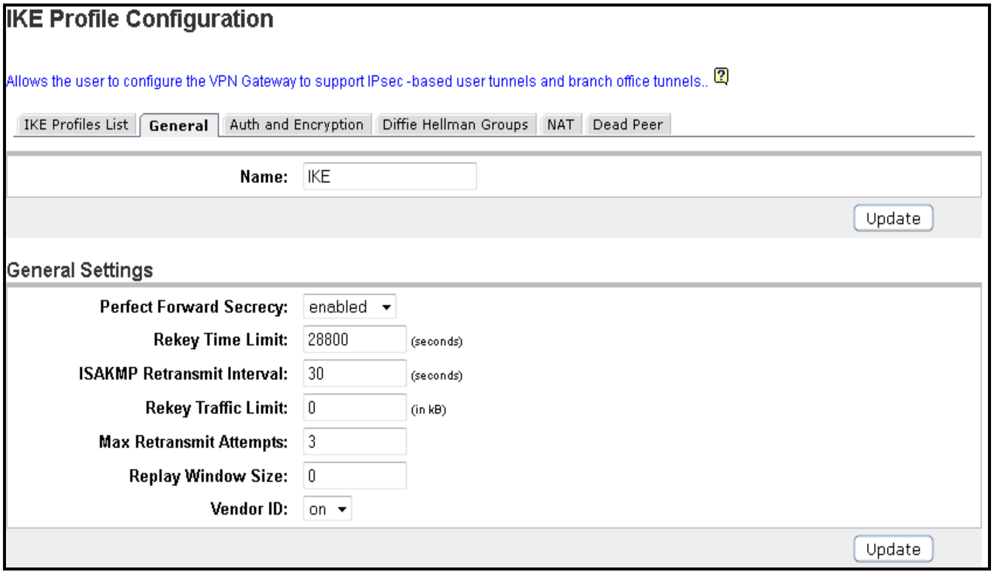
Id: 2

Name:

7. **In the Name field, enter a name for the IKE profile.**

8. **Click Update.**

   The IKE Profile Configuration form is redisplayed with new IKE profile.



IKE Profile Configuration

Allows the user to configure the VPN Gateway to support IPsec -based user tunnels and branch office tunnels..

Name: IKE

General Settings

Perfect Forward Secrecy: enabled

Rekey Time Limit: 28800 (seconds)

ISAKMP Retransmit Interval: 30 (seconds)

Rekey Traffic Limit: 0 (in kB)

Max Retransmit Attempts: 3

Replay Window Size: 0

Vendor ID: on

Use the General, Auth and Encryption, Diffie-Hellman Group, NAT and Dead Peer forms to modify the IKE profile according to your needs.

9. **Enables the Perfect Forward Secrecy (PFS) feature. With PFS enabled, keys are not derived from previous keys. This ensures that one key being compromised cannot result in the compromise of subsequent keys.**

   The default value is `enabled`.

10. **Sets the maximum lifetime of the single session key. The setting controls how often new session keys are exchanged between the client and the Avaya VPN Gateway device. Limiting the lifetime of a single key used to encrypt data is a way of increasing session security. Set the limit to no less than 1 hour.**

    The default value is 8h (8 hours). The maximum setting is 23h59m59s(23 hours,59 minutes and 59 seconds). A setting of 0 seconds disables the setting.

11. **Sets the time interval after which the IKE packet is assumed to be lost and is retransmitted.**

12. **Sets the maximum traffic allowed before new session keys are exchanged between the client and Avaya VPN Gateway device.**

    The default value is 0 Kbytes. A setting of 0 disables the setting.

13. **Sets the maximum number of retransmissions. This is the number of times that the client retransmits a keepalive packet to the Avaya VPN Gateway device to check for connectivity.**

14. **Provides a way to define the accepted range of sequence numbers. While the default handling calls for the sender to increment the sequence number used for anti-replay, the service is effective only if the receiver checks the sequence number.**

    The default value is 0, which disables the anti-replay service.

15. **Enables Vendor Id Transmission.**

    Default is on.

    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.

16. **Click Update and Apply the changes.**

17. **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 Branch office tunnel profile menu, see the `botunprof` command in the *User's Guide*.

1. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form is displayed.

2. **Select the configured VPN for which you to create a Branch Office Tunnel Profile.**

   The VPN Summary form is displayed.

3. **Under Settings, select IP Sec.**

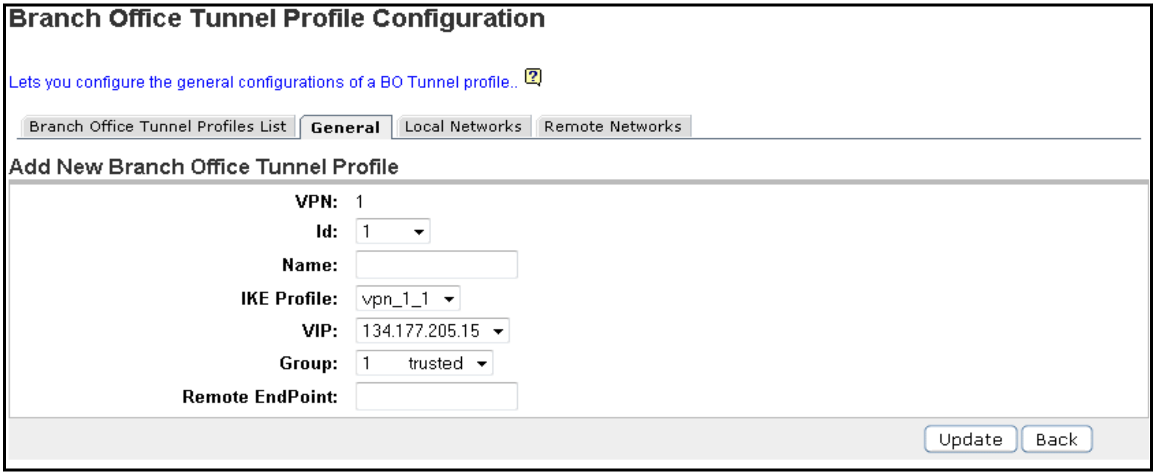
   The General form is displayed.

4. **Select BO Tunnel Profiles.**

   The Branch Office Tunnel Profiles form is displayed.

5. **Click Add.**

The Add New Branch Office Tunnel Profile form is displayed.



Branch Office Tunnel Profile Configuration

Lets you configure the general configurations of a BO Tunnel profile..

Add New Branch Office Tunnel Profile

VPN: 1

Id: 1

Name:

IKE Profile: vpn_1_1

VIP: 134.177.205.15

Group: 1 trusted

Remote EndPoint:

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. You should previously have configured one or several Portal IP addresses (or VIPs) for the current VPN under **VPN Gateways>VPN #>IP Addresses**.

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 Avaya VPN Gateway.

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.

    The Branch Office Tunnel Profile Configuration form is displayed.

11. **Click Update.**

Shared Secret Authentication

The authentication type is set to sharedsecret by default. As an alternative, the authentication type can be set to cert (see following section "Certificate Authentication" on page 552).

1. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form is displayed.

2. **Select the configured VPN for which you to create a Branch Office Tunnel Profile.**

   The VPN Summary form is displayed.

3. **Under Settings, select IP Sec.**

   The General form is displayed.

4. **Select BO Tunnel Profiles.**

   The Branch Office Tunnel Profiles form is displayed.

5. **In the Authentication Type list box, verify that shared secret is selected.**

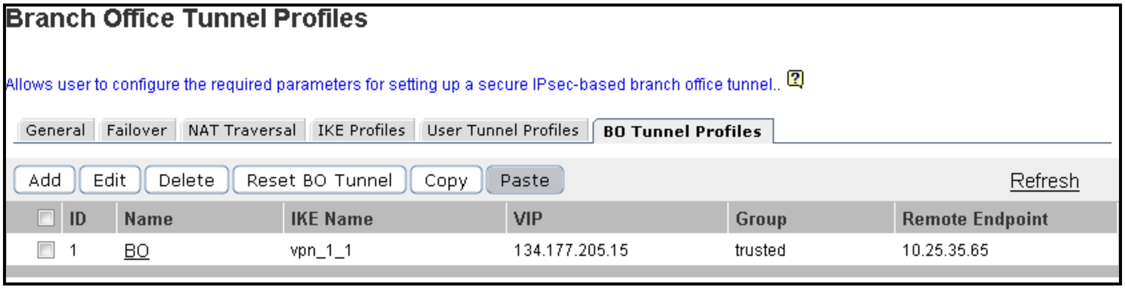
6. **In the Shared Secret fields, enter the shared secret.**

   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.**

8. **Select Branch Office Tunnel Profiles List.**

   The branch office tunnel profile is added to the list.



Branch Office Tunnel Profiles

Allows user to configure the required parameters for setting up a secure IPsec-based branch office tunnel..

□	ID	Name	IKE Name	VIP	Group	Remote Endpoint
□	1	BO	vpn_1_1	134.177.205.15	trusted	10.25.35.65

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 an Avaya 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.

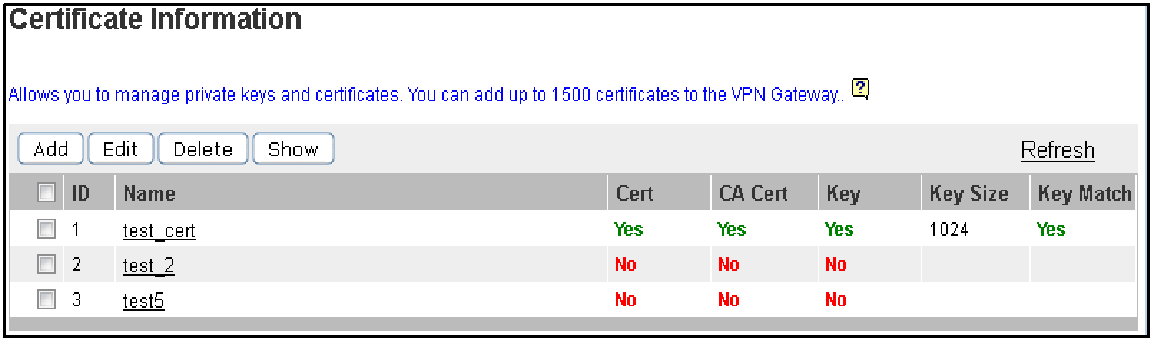
1. **In the System tree view, expand BO Tunnel Profiles and select Branch Office Tunnel Profiles.**

   The Branch Office Tunnel Profile Configuration form is displayed.

2. **In the Authentication Type list box, set the authentication type to `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 Avaya VPN Gateway you could find out the OIDs and their values for the certificate under **Certificates>Show**.



Certificate Information

Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway.

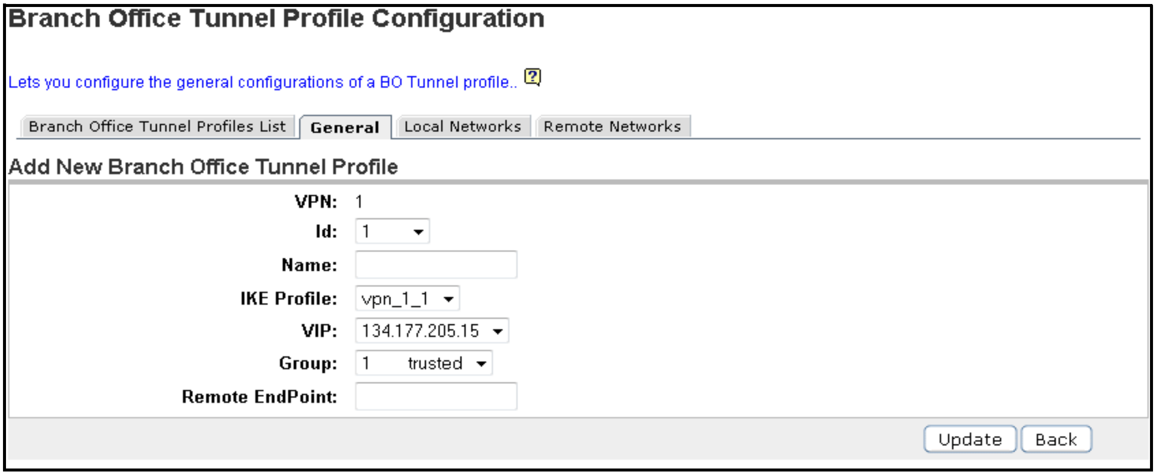
□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		

   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 would be `Testing`.



Branch Office Tunnel Profile Configuration

Lets you configure the general configurations of a BO Tunnel profile..

Add New Branch Office Tunnel Profile

VPN:	1
Id:	1
Name:	
IKE Profile:	vpn_1_1
VIP:	134.177.205.15
Group:	1 trusted
Remote EndPoint:	

The Quick Choice list box contains some suggestions for symbolic names (representing certificate OIDs) that can be used to extract a value from the remote certificate. Symbolic names can be entered in the Remote Certificate OID field as well as OID numbers.

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 Avaya VPN Gateway to the remote endpoint.

   To be able to select the certificate, it must exist on the Avaya 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 Avaya 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

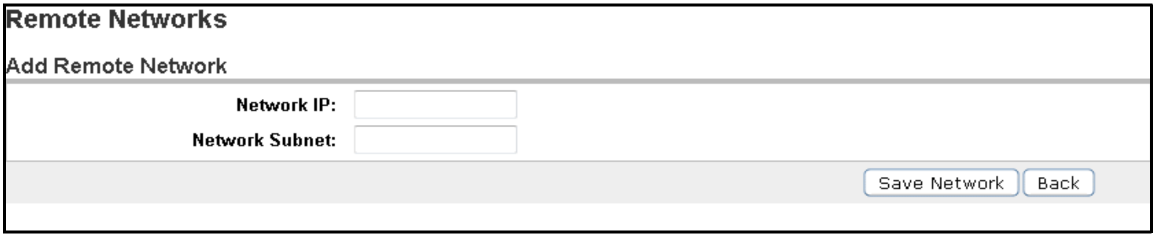
This step lets you configure the remote (branch office) networks that should be accessible through the branch office tunnel.

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 is displayed.



Remote Networks

Add Remote Network

Network IP:

Network Subnet:

3. **Click Add.**

   The Add Remote Network form is displayed.

4. **In the Network IP field, enter a remote 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.**

7. **The network is added to the Remote Networks list.**

8. **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 Branch Office Tunnel Profile, select the BO tunnel for which you wish to configure local networks.**

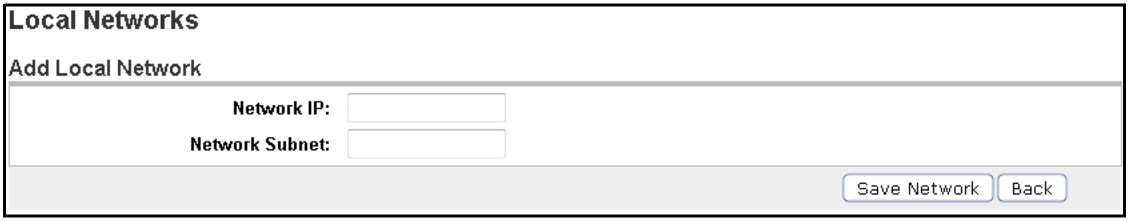
   The Branch Office Tunnel Profile Configuration is displayed.

2. **Select Local Networks.**

The Local Networks form is displayed.

3. **Click Add.**

   The Add Local Network form is displayed.



Local Networks

Add Local Network

Network IP:	
Network Subnet:	

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.**

7. **The network is added to the Local Networks list.**

8. **Add additional networks in the same way if needed.**

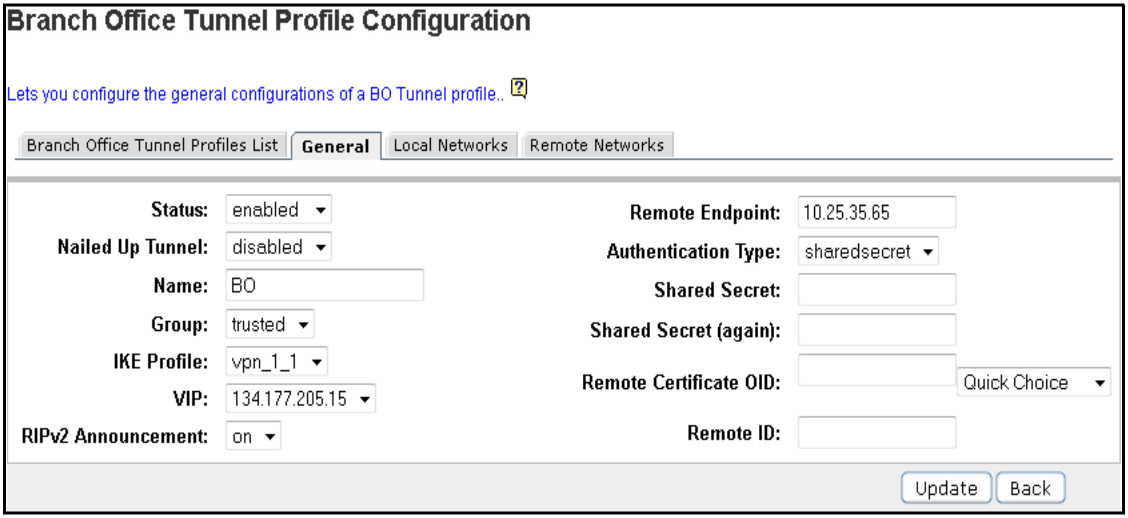
9. **Apply the changes.**

   For an explanation of BO Tunnel Profile menu options that have not been covered in this document, see the *User's Guide*.

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.**



Branch Office Tunnel Profile Configuration

Lets you configure the general configurations of a BO Tunnel profile..

Status: enabled

Nailed Up Tunnel: disabled

Name: BO

Group: trusted

IKE Profile: vpn_1_1

VIP: 134.177.205.15

RIPv2 Announcement: on

Remote Endpoint: 10.25.35.65

Authentication Type: sharedsecret

Shared Secret:

Shared Secret (again):

Remote Certificate OID: Quick Choice

Remote ID:

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 Avaya VPN Gateways.
   - `off`: Branch office networks are not announced on the private side. This setting may cause routing problems when the cluster consists of several Avaya VPN Gateways.
   - `all`: Same as `on` but the announcement is made on all interfaces.

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

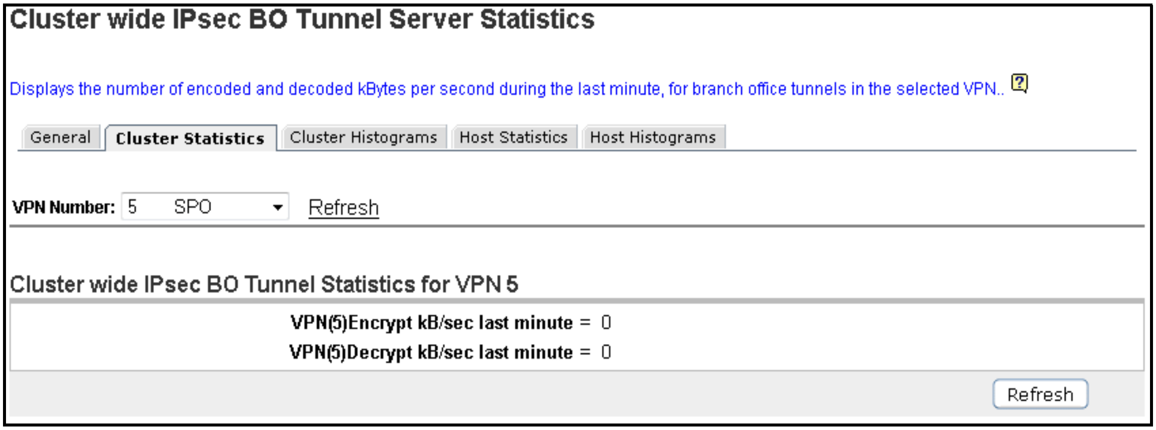
Branch Office Tunnel Statistics

To view branch office tunnel statistics, proceed as follows:

1. **In the System tree view, expand Monitor, Statistics and IPsec.**
2. **Under IPsec, select BO Tunnels.**

   Here you will find different options for viewing branch office tunnel performance statistics. The information can be shown on a cluster-wide level, per Avaya VPN Gateway host, per VPN and so on.

Following is an example of the cluster-wide branch office tunnel server statistics screen.



Cluster wide IPsec BO Tunnel Server Statistics

Displays the number of encoded and decoded kBytes per second during the last minute, for branch office tunnels in the selected VPN..

VPN Number: 5 SPO Refresh

Cluster wide IPsec BO Tunnel Statistics for VPN 5

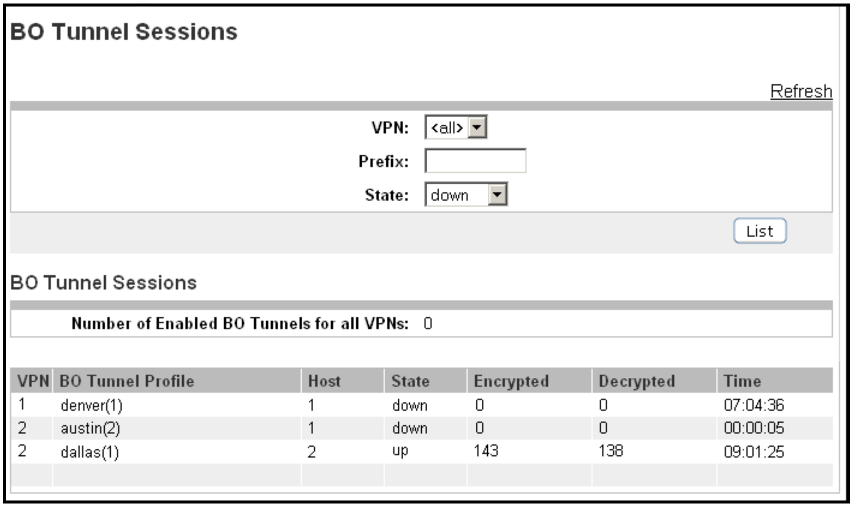
VPN(5)Encrypt kB/sec last minute = 0
VPN(5)Decrypt kB/sec last minute = 0

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.**



BO Tunnel Sessions

VPN: <all>
Prefix:
State: down

BO Tunnel Sessions

Number of Enabled BO Tunnels for all VPNs: 0

VPN	BO Tunnel Profile	Host	State	Encrypted	Decrypted	Time
1	denver(1)	1	down	0	0	07:04:36
2	austin(2)	1	down	0	0	00:00:05
2	dallas(1)	2	up	143	138	09:01:25

The output shows the name of the branch office tunnel profile, the Avaya VPN Gateway 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 e.g. `d*`.

To limit the view to BO tunnels in a specific state, select the desired state in the State list box.

CHAPTER 19

Layer 2 Tunneling Protocol

This chapter provides procedures to configure the Avaya VPN Gateway device for Layer 2 Tunneling Protocol (L2TP).

Overview

The Layer 2 Tunneling Protocol acts as a data link layer protocol for tunneling network traffic between two peers over an existing network or Internet. The protocol uses the registered User Datagram Protocol (UDP) port 1701. The L2TP packet, including payload and L2TP header, is sent within a UDP datagram. L2TP does not provide confidentiality or strong authentication by itself; IPsec is used to secure L2TP packets by providing confidentiality, authentication, and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

An L2TP tunnel has two end points, LAC (L2TP Access Concentrator) and the LNS (L2TP Network Server). The LAC is the initiator of the tunnel and the LNS is the server, which waits for new tunnels. When the system starts, the tunnels get automatically established, and the network traffic between the peers is bidirectional. User tunnels use a previously configured Internet Key Exchange (IKE) profile. The IKE profile includes the preferred encryption settings for the tunnel.

As part of the IKE (ISAKMP) protocol, AVG authenticates the end user or road warrior to ensure that IKE SAs are established with the intended party using the Digital Certificate and Preshared Key (PSK) authentication.

Digital Certificate: In this authentication, a pair of private key and public key are used to authenticate the peer. The initiator signs the message interchange data using a private key, and shares the public key with the responder through messages (certificate request and certificate response) containing an X.509 certificate. The responder uses this public key to verify the signature. The X.509 certificate provides a level of assurance that identity of the peer —as represented in the certificate— is associated with a particular public key.

PreShared Key: This method is used to authenticate end user PC. In this authentication, a secret key is shared between AVG and end user PC. The same secret key must be configured on both AVG and end user PC before both machines can authenticate each other.

After establishing the L2TP tunnel, Peer-to-Peer Protocol is used for user authentication and tunnel interface set up. The supported user authentication protocols are MSCHAPv2, MSCHAPv1, PAP, and CHAP.

After configuring and enabling L2TP VPN on AVG, clients such as Windows or Mac L2TP clients can connect to AVG.

To configure L2TP, see the following:

1. **"Enabling L2TP" on page 561**
2. **"Configure IKE Profile" on page 562**
3. **"Configure User Tunnel Profile" on page 572**
4. **"Creating the IP Pool" on page 574**
5. **"Creating default IP Pool" on page 579**
6. **"Mapping the IP Pool" on page 579**
7. **"Selecting Authentication Order" on page 580**
8. **"Configuring L2TP connection for Windows client" on page 581**
9. **"Configuring L2TP connection for iPhone client" on page 583**
10. **"Configuring L2TP connections for Android" on page 585**

Enabling L2TP

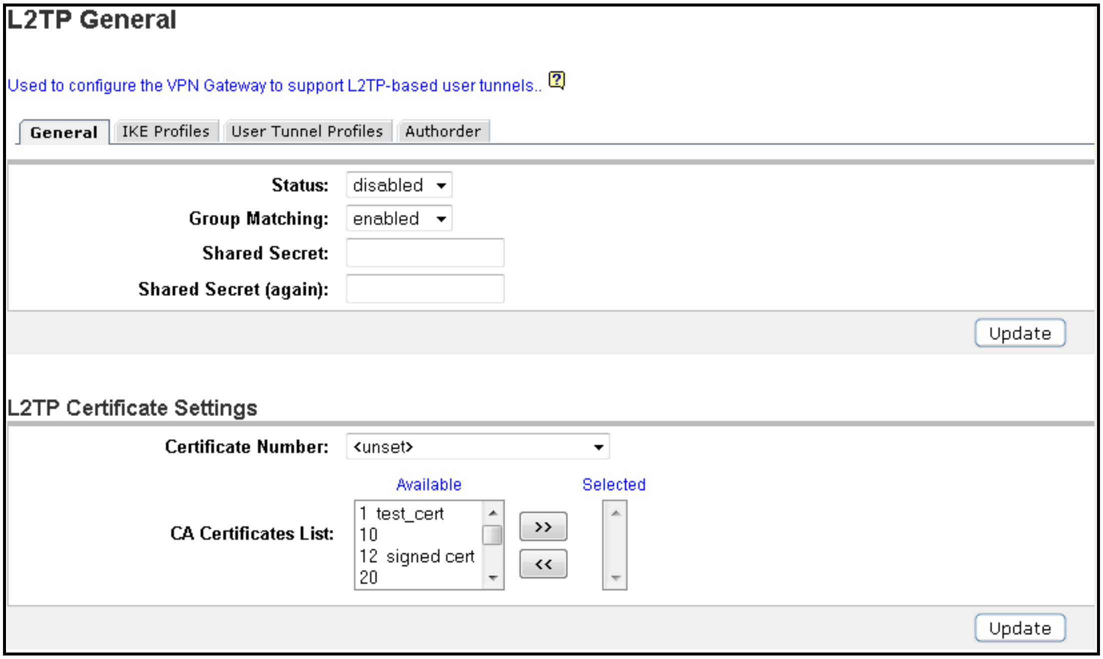
To enable L2TP, perform the following:

1. **Log on to the BBI as an administrator user.**
2. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to enable L2TP.**

   The VPN Summary form appears.
4. **Select L2TP.**

   The General form appears.



L2TP General

Used to configure the VPN Gateway to support L2TP-based user tunnels..

Status: disabled

Group Matching: enabled

Shared Secret:

Shared Secret (again):

L2TP Certificate Settings

Certificate Number: <unset>

CA Certificates List:

Available	Selected
1 test_cert 10 12 signed cert 20	

5. **Click the General tab.**
6. **From the Status list, select enabled.**
7. **From the Group Matching list, select enabled.**
8. **In the Shared Secret field, enter the shared secret.**
9. **In the Shared Secret (again) field, enter the shared secret to reconfirm.**

10. **Select the RADIUS binding value from the pull-down menu.**
    - `Enabled` activates the feature
    - `Disabled` de-activates the feature
11. **Click Update.**
12. **From the Certificate Number list, select the certificate number for the L2TP server.**
13. **From the CA Certificate List field, select the certificate for client authentication.**

NOTE – If Certificates are used for authentication, a valid CA certificate must be configured in the accepted CA list on AVG.

---

14. **Click Update.**
15. **Click Apply.**

Configure IKE Profile

See the following to configure IKE profile:

- "Creating an IKE Profile" on page 562
- "Configuring dead peer" on page 566
- "Configuring Diffie-Hellman Groups" on page 569
- "Configuring NAT" on page 570

Creating an IKE Profile

To create an IKE profile with different settings for encryption, perform the following:

1. **Log on to the BBI as an administrator user.**
2. **In the System tree view, select VPN Gateways.**

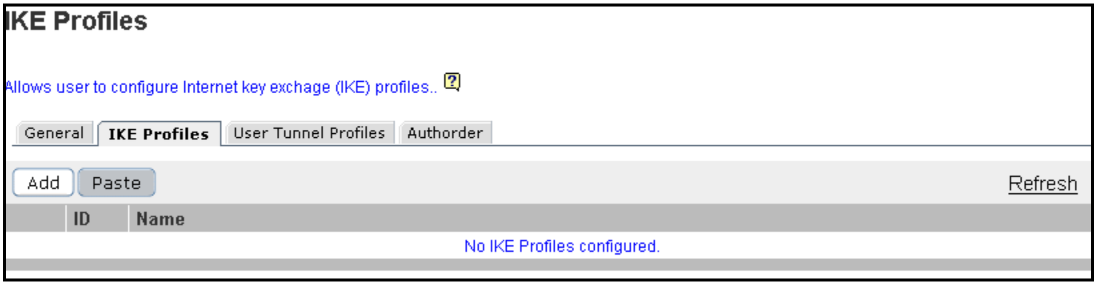
   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to create an IKE profile.**

   The VPN Summary form appears.
4. **Select L2TP.**

   The General form appears.

5. **Click the IKE Profiles tab.**

   The IKE Profiles form appears.



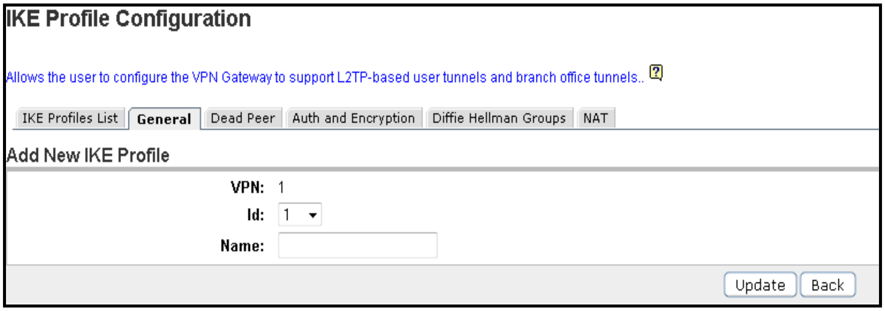
IKE Profiles

Allows user to configure Internet key exchange (IKE) profiles..

ID	Name
No IKE Profiles configured.	

6. **Click Add.**

   The Add New IKE Profile form appears.



IKE Profile Configuration

Allows the user to configure the VPN Gateway to support L2TP-based user tunnels and branch office tunnels..

Add New IKE Profile

VPN: 1

Id: 1

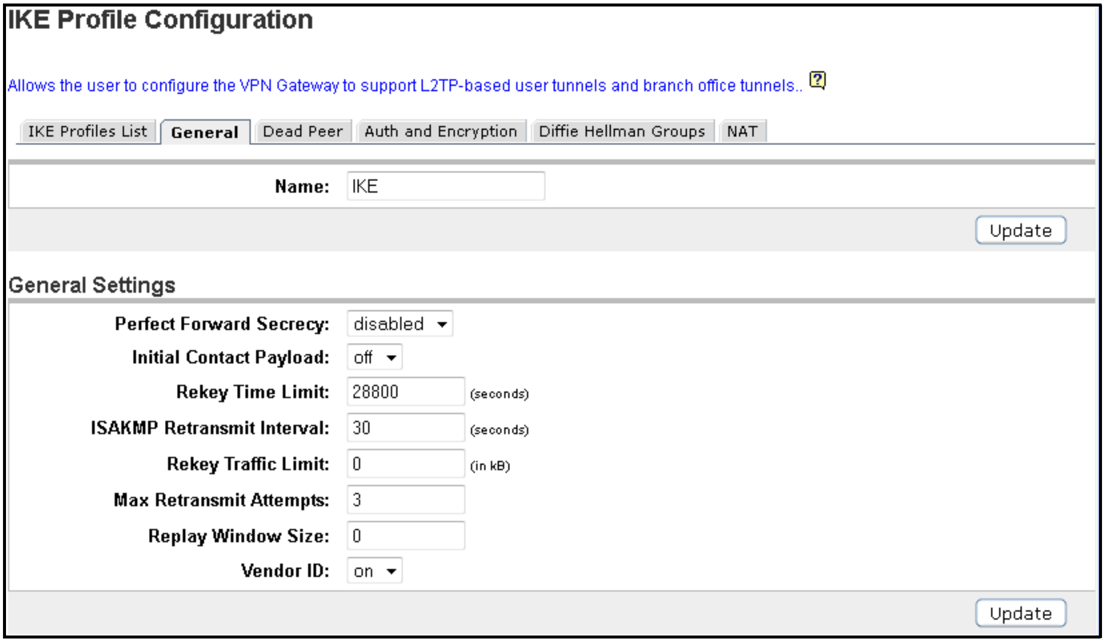
Name:

7. **From the ID list, select ID.**

8. **In the Name field, enter a name for the IKE profile.**

9. **Click Update.**

The IKE Profile Configuration form reappears with the new IKE profile.



IKE Profile Configuration

Allows the user to configure the VPN Gateway to support L2TP-based user tunnels and branch office tunnels..

Name: IKE

General Settings

Perfect Forward Secrecy: disabled
Initial Contact Payload: off
Rekey Time Limit: 28800 (seconds)
ISAKMP Retransmit Interval: 30 (seconds)
Rekey Traffic Limit: 0 (in kB)
Max Retransmit Attempts: 3
Replay Window Size: 0
Vendor ID: on

Use the General, Dead Peer, Auth and Encryption, Diffie-Hellman Group, and NAT forms to modify the IKE profile.

10. **From the Perfect Forward Secrecy list, select enabled.**

    Keys are not derived from previous keys when you enable Perfect Forward Secrecy (PFS). This ensures even if one key is compromised, the subsequent keys are not compromised.

11. **From the Initial Contact Payload list, select on.**

12. **In the Rekey Time Limit field, enter the maximum lifetime of the single session key.**

    Rekey limit controls how often new session keys are exchanged between the client and the Avaya VPN Gateway device. You can increase the session entry to limit the lifetime of a single key used to encrypt data. The limit must not be less than 1 hour.

    The default value is 8h (8 hours). The maximum setting is 23h59m59s (23 hours, 59 minutes, and 59 seconds). A setting of 0 disables the setting.

13. **In the ISAKMP Retransmit Interval field, enter the time interval for retransmitting the IKE packet.**

14. **In the Rekey Traffic Limit field, enter the maximum traffic allowed before new session keys are exchanged between the client and the Avaya VPN Gateway device.**

    The default value is 0 Kbyte. The value 0 disables the setting.

15. **In the Max Retransmit Attempts field, enter the maximum number of retransmissions.**

    Maximum attempts a client tries to retransmit the keepalive packet to the Avaya VPN Gateway device to check for connectivity.

16. **In the Replay Window Size field, enter the accepted range of sequence numbers.**

    Default handling calls for the sender increments the sequence number used for the antireplay. The default setting is effective only if the receiver checks the sequence number.

    The default value is 0. The value 0 disables the antireplay service.

17. **From the Vendor ID list, select on.**

    The default value is on.

18. **Click Update.**

19. **In the Name section, click Update.**

Configuring dead peer

Use Dead Peer menu to detect tunnel failure due to connectivity loss. Avaya VPN Gateway assumes the connectivity is lost if it does not receive L2TP traffic and keep alive messages from the client. To configure dead peer, perform the following steps:

1. **From the System tree view, select VPN Gateways**

   The VPN Gateways screen appears.

2. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

3. **Select the configured VPN for which you want to create an IKE profile.**

   The VPN Summary form appears.

4. **Select L2TP.**

   The General form appears.

5. **Click the IKE Profiles tab.**

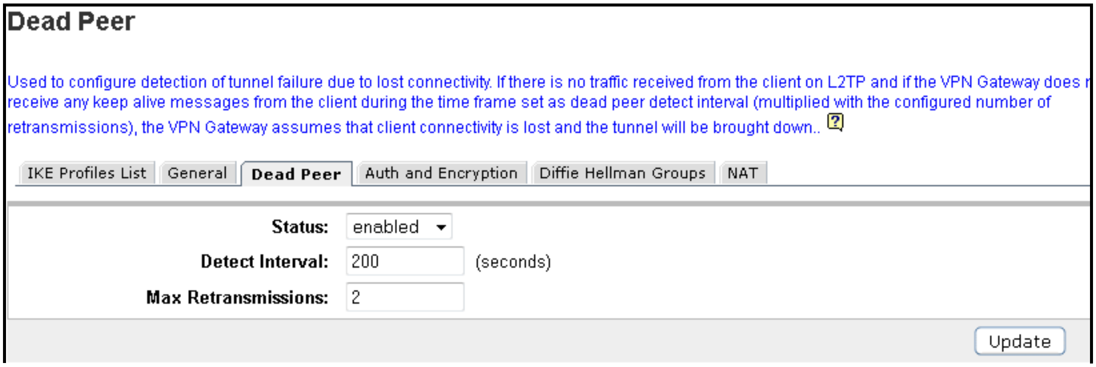
   The configured IKE Profiles appears

6. **Select the IKE profile.**

   The IKE Profile Add/Update form appears.

7. **Click the Dead Peer.**

   The Dead Peer form appears.



Dead Peer

Used to configure detection of tunnel failure due to lost connectivity. If there is no traffic received from the client on L2TP and if the VPN Gateway does r
receive any keep alive messages from the client during the time frame set as dead peer detect interval (multiplied with the configured number of retransmissions), the VPN Gateway assumes that client connectivity is lost and the tunnel will be brought down..

Status: enabled

Detect Interval: 200 (seconds)

Max Retransmissions: 2

8. **From the Status list, select enabled.**

9. **In the Detect Interval field, enter the waiting time period in seconds to check the receipt of keep alive messages from the L2TP client.**

10. **In Max Retransmissions field, enter the maximum number of times the AVG device checks the receipt of keep alive messages from the L2TP client.**

11. **Click Update.**

12. **Apply the changes.**

Configuring Authentication and Encryption

The authentication and encryption form configures the encryption parameters for the selected IKE profile.

To configure authentication and encryption, perform the following procedure:

1. **From the System tree view, select VPN Gateways**

   The VPN Gateways screen appears.

2. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

3. **Select the configured VPN for which you want to create an IKE profile.**

   The VPN Summary form appears.

4. **Select L2TP.**

   The General form appears.

5. **Click the IKE Profiles tab.**

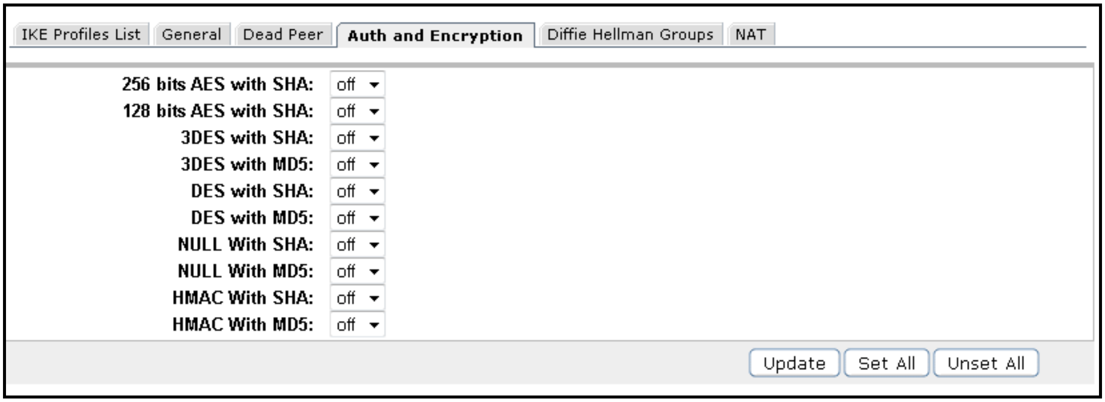
   The configured IKE Profiles appears

6. **Select the IKE profile.**

   The IKE Profile Add/Update form appears.

7. **Click the Authentication and Encryption tab.**

   The Authentication and Encryption form appears.



256 bits AES with SHA:	off
128 bits AES with SHA:	off
3DES with SHA:	off
3DES with MD5:	off
DES with SHA:	off
DES with MD5:	off
NULL With SHA:	off
NULL With MD5:	off
HMAC With SHA:	off
HMAC With MD5:	off

8. **From the 256 bits AES with SHA list, select on or off to enable or disable 256 bit Advanced Encryption Standard (AES).**

9. **From the 128 bits AES with SHA list, select on or off to enable or disable 128 bit Advanced Encryption Standard (AES).**

10. **From the 3DES with SHA list, select on or off to enable or disable 3 Data Encryption Standard (DES) with Secure Hash Algorithm (SHA) encryption.**

11. **From the 3DES with MD5 list, select on or off to enable or disable 3DES with Message Digest (MD) 5 encryption.**

12. **From the DES with SHA list, select on or off to enable or disable DES with SHA encryption.**

13. **From the DES with MD5 list, select on or off to enable or disable DES with MD5 encryption.**

14. **From the Null With SHA list, select on or off to enable or disable NULL With SHA encryption.**

15. **From the Null With MD5 list, select on or off to enable or disable NULL With MD5 encryption.**

16. **From the HMAC With SHA list, select on or off to enable or disable Hash Message Authentication Code (HMAC) With SHA encryption.**

17. **From the HMAC With MD5 list, select on or off to enable or disable HMAC With MD5 encryption.**

18. **Click Update.**

Configuring Diffie-Hellman Groups

Use the Diffie-Hellman form to enable or disable the desired Diffie-Hellman group settings for the selected IKE profile. To configure Diffie-Hellman group, perform the following steps:

1. **From the System tree view, select VPN Gateways**

   The VPN Gateways screen appears.

2. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

3. **Select the configured VPN for which you want to create an IKE profile.**

   The VPN Summary form appears.

4. **Select L2TP.**

   The General form appears.

5. **Click the IKE Profiles tab.**

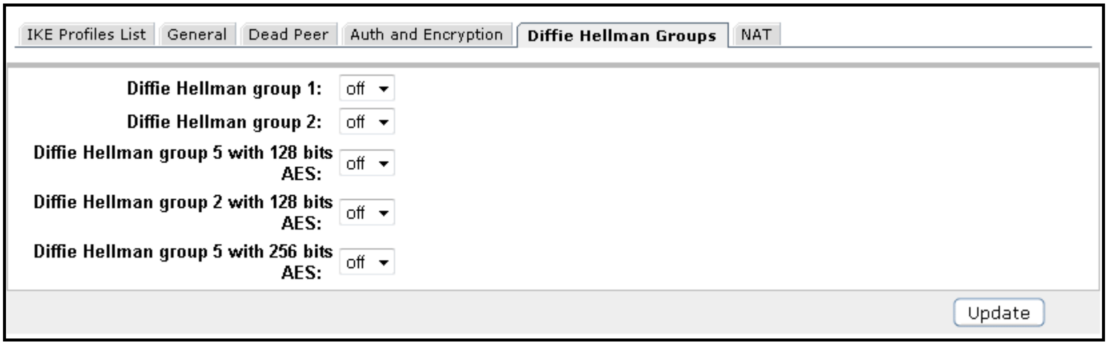
   The configured IKE Profiles appears

6. **Select the IKE profile.**

   The IKE Profile Add/Update form appears.

7. **Click the Diffie-Hellman Groups.**

   The Diffie-Hellman Groups form appears.



Diffie Hellman group 1: off

Diffie Hellman group 2: off

Diffie Hellman group 5 with 128 bits AES: off

Diffie Hellman group 2 with 128 bits AES: off

Diffie Hellman group 5 with 256 bits AES: off

8. **From the Diffie Hellman group 1 list, select on or off to enable or disable Diffie Hellman group 1.**

9. **From the Diffie Hellman group 2 list, select on or off to enable or disable Diffie Hellman group 2.**

10. **From the Diffie Hellman group 5 list, select on or off to enable or disable Diffie Hellman group 5.**

11. **From the Diffie Hellman group 2 with AES list, select on or off to enable or disable Diffie Hellman group 2 with AES.**

12. **From the Diffie Hellman group 5 with AES list, select on or off to enable or disable Diffie Hellman group 5 with AES.**

13. **Click Update.**

Configuring NAT

The Layer 2 Tunneling Protocol aware Network Address Translation (NAT) devices handle L2TP traffic but if the NAT device is not L2TP aware, then the client PC and the Avaya VPN Gateway device can negotiate to encapsulate the L2TP packets within the UDP. Use the NAT menu to configure NAT device detection and packet encapsulation.

To configure NAT, perform the following steps:

1. **In the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.

2. **Select the configured VPN for which you want to create an IKE profile.**

   The VPN Summary form appears.

3. **Select L2TP.**

   The General form appears.

4. **Click the IKE Profiles tab.**

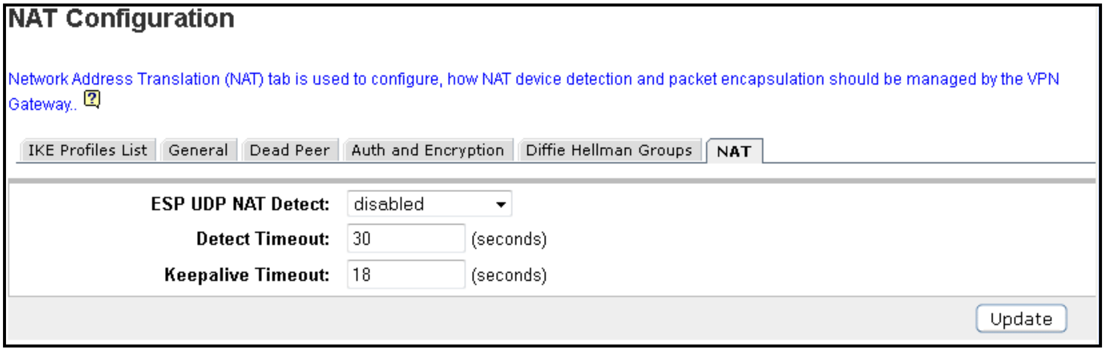
   The configured IKE Profiles appears

5. **Select the IKE profile.**

   The IKE Profile Add/Update form appears.

6. **Click the NAT tab.**

The NAT form appears.



NAT Configuration

Network Address Translation (NAT) tab is used to configure, how NAT device detection and packet encapsulation should be managed by the VPN Gateway.. ?

ESP UDP NAT Detect: disabled

Detect Timeout: 30 (seconds)

Keepalive Timeout: 18 (seconds)

7. **From the ESP UDP NAT Detect list, select one of the following:**

   disabled – does not encapsulate the L2TP packets within the UDP even if a NAT device is detected.

   Or

   auto – encapsulates the L2TP packets within the UDP.

   Or

   ipsec_capable – initially does not encapsulate the L2TP packets within the UDP. The L2TP forwarding subsystem checks for traffic on the L2TP Security Association (SA). If the NAT device does not forward the L2TP traffic on the L2TP SA, a UDP encapsulation is required. The L2TP forwarding subsystem sends a rekey initiation to IKE for initiating a new L2TP SA to encapsulate the L2TP packets within the UDP.

   Or

   use_udp_encap – this is the implementation of RFC 3948. When NAT is detected, IKE traffic uses UDP port 4500 for completing the further ISAKMP handshakes. After establishing the Security Association, IPsec traffic is encapsulated in the UDP port. A non ESP marker header separates IKE traffic from IPsec traffic on the UDP port.In the Detect Timeout field, enter the timeout value for NAT in seconds. The default value is 0.

8. **Click Update.**

9. **Apply the changes.**

Configure User Tunnel Profile

You can use the default settings for the user tunnel profile with the L2TP. For more information about the available settings, see *User's Guide* (NN46220-103).

To define different criteria for L2TP user tunnel, perform the following steps:

1. **From the System tree view, select VPN Gateways**

   The VPN Gateways screen appears.

2. **Select the configured VPN for which you want to enable User Tunnel Profile.**

   The VPN Summary screen appears.

3. **Select L2TP.**

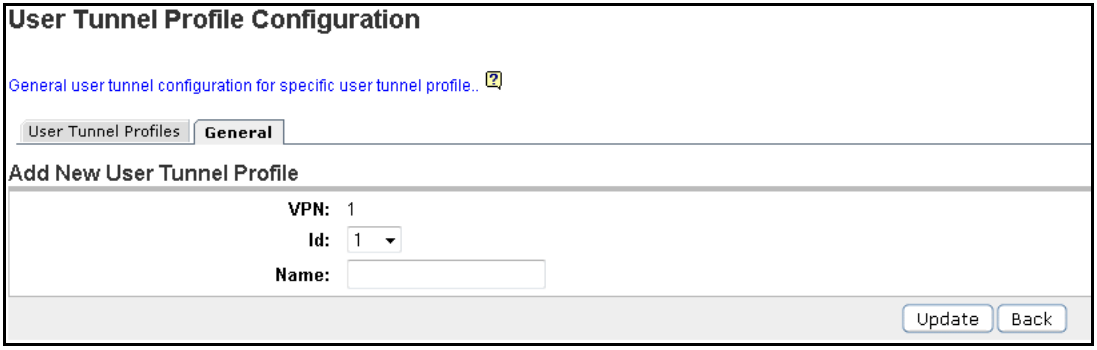
   The General screen appears.

4. **Select User Tunnel Profiles tab.**

   The User Tunnel Profiles screen appears.

5. **Click Add.**

   The Add New User Tunnel Profile form appears.



User Tunnel Profile Configuration

General user tunnel configuration for specific user tunnel profile..

Add New User Tunnel Profile

VPN: 1

Id: 1

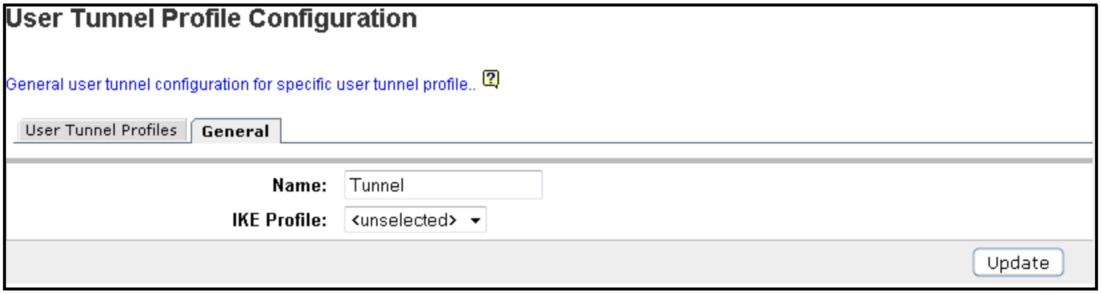
Name:

6. **From the ID list, select the ID.**

7. **In the Name field, enter a name for the user tunnel profile.**

8. **Click Update.**

The General form appears.



User Tunnel Profile Configuration

General user tunnel configuration for specific user tunnel profile..

Name: Tunnel

IKE Profile: <unselected>

9. **From the IKE Profile list, select the previously created IKE profile.**

10. **Click Update.**

11. **Apply the changes.**

Creating the IP Pool

The IP Pool is used when the remote user tries to access a host using the L2TP VPN client. After creating the IP Pool, the AVG assigns the new IP address as a source IP for the unencrypted connection between the Avaya VPN Gateway and the destination host. You can also define specific network attributes for this connection. You can configure several IP Pools, each with a unique ID number with unique properties. By mapping the desired IP Pool to a user group, you can create different methods for IP address and assign network attributes for different user groups.

Select one of the configured IP Pools as the default IP Pool. Groups with no IP Pool are assigned default IP Pool (IP Pool number=0).

To configure the IP Pool, perform the following steps:

1. **From System tree view, select VPN Gateways.**

   The VPN Gateways screen appears.

2. **Select the configured VPN for which you want to enable the IP Pool.**

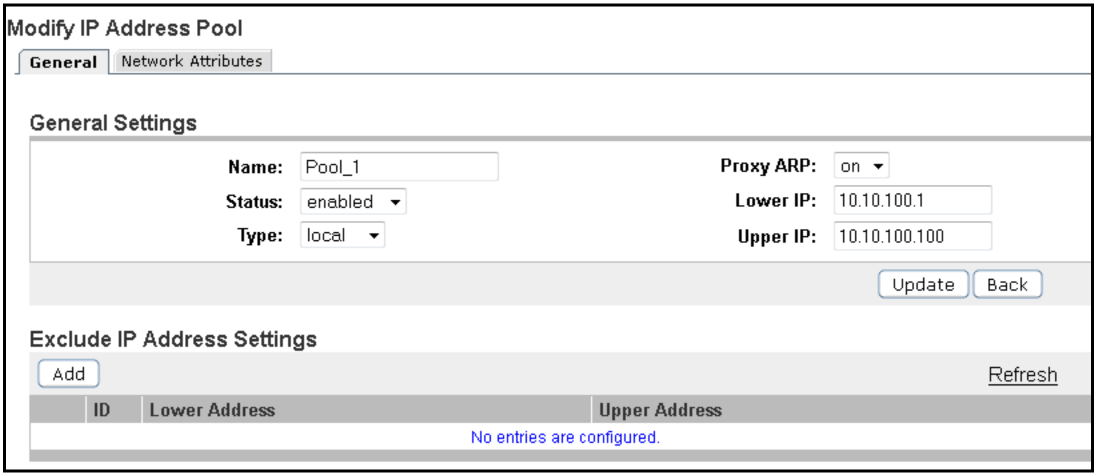
   The VPN Summary screen appears.

3. **Select the IP Pool.**

   The IP Pool form appears.

4. **Click Add.**

The IP Pool Configuration form appears. The first available IP Pool number appears in the IP Pool ID list.



Modify IP Address Pool

General Settings

Name:	Pool_1	Proxy ARP:	on
Status:	enabled	Lower IP:	10.10.100.1
Type:	local	Upper IP:	10.10.100.100

Exclude IP Address Settings

	ID	Lower Address	Upper Address

No entries are configured.

5. **In the Name field, enter a name for the IP Pool.**

6. **From the Status list, select enabled to enable the IP Pool.**

   You can disable the IP Pool without losing the other settings for the Pool and also re-enable the IP Pool with the configurations.

7. **From the Type list, select the local, radius, or dhcp network attribute.**

   You can assign network attributes (including IP address) either locally (from the Avaya VPN Gateway) from an external RADIUS server or from an external DHCP server.

   Configure network attributes for IP Pools of the `local` type on the Avaya VPN Gateway. You can configure network attributes IP Pools of the `radius` and `dhcp` types on the Avaya VPN Gateway as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute.

8. **In the Proxy ARP list, select one of the following:**

   yes, to enable the IP address for a specific client connection and respond to ARP requests on behalf of the L2TP VPN client for return traffic

   Or

   no, to disable the return traffic to reach its destination unless specific routes are configured

   Or

all, to enable the IP address for a specific client connection without proxy ARP on all interfaces

9. **Click Update.**

Different entry forms appear depending on the selected IP Pool mechanism (`local`, `radius` or `dhcp`). Perform the following procedures according to your IP Pool configuration selection:

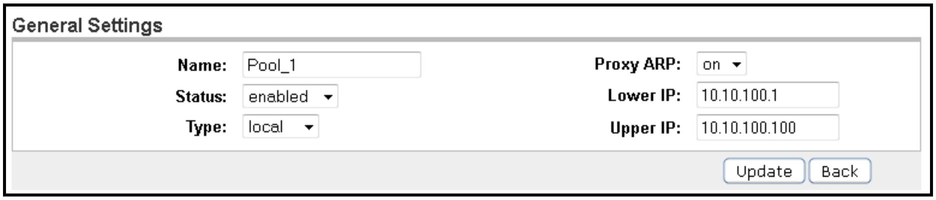
- “Configuring IP address range and local network attributes” on page 576
- “Configuring RADIUS network attributes” on page 577
- “Configuring DHCP Network Attributes” on page 578

Configuring IP address range and local network attributes

To configure the desired IP address range for local network attribute, perform the following:

1. **Click the General Settings tab.**

The General Settings form appears.



General Settings

Name: Pool_1

Status: enabled

Type: local

Proxy ARP: on

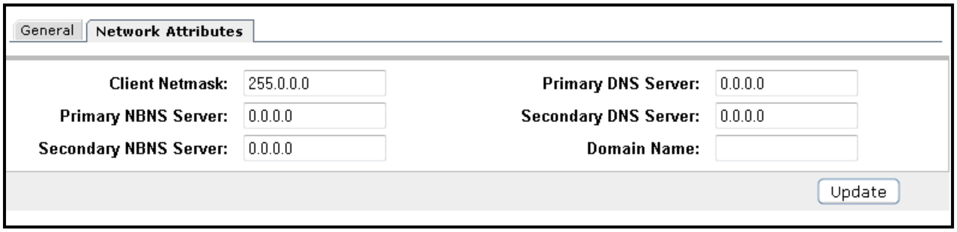
Lower IP: 10.10.100.1

Upper IP: 10.10.100.100

2. **In the Lower IP and Upper IP field, enter the IP address.**

3. **Click the Network Attributes tab.**

The Network Attributes Settings form appears.



Client Netmask: 255.0.0.0

Primary NBNS Server: 0.0.0.0

Secondary NBNS Server: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Domain Name:

4. **In the Client Netmask field, enter the network mask for the client.**

The network mask must cover the IP address range specified in Step 1. The default network mask is `255.255.255.0`.

5. **In the Primary NBNS Server field, enter the IP address of a primary NBNS server (NetBIOS Name Server).**

   Specify the primary NetBIOS Name Service (NBNS) Server IP address if the L2TP VPN client must use a specific NBNS server to contain computer names resolved into IP addresses. NetBIOS Name Service servers provide Windows Internet Naming Service (WINS), which is part of the Microsoft Windows NT server environment.

6. **In the Secondary NBNS Server field, enter the IP address of a secondary NBNS server.**

7. **In the Primary DNS Server field, enter the IP address of a primary DNS server.**

   Specify the primary DNS server IP address if the L2TP VPN client must use a specific DNS server to contain domain names resolved into IP addresses. The DNS server of the remote user VPN is used if the primary DNS server is not specified.

8. **In the Secondary DNS Server field, enter the IP address of a secondary DNS server.**

9. **In the Domain Name field, enter the name of the domain used while creating the L2TP user tunnel.**

   The domain name ensures that the domain lookup operations point to the correct domain. This domain lookup is particularly important for clients using Microsoft Outlook or Exchange.

10. **Click Update.**

Configuring RADIUS network attributes

The RADIUS network attributes, for example primary or secondary DNS server, you can retrieve the primary or secondary NBNS server from the RADIUS server. You can also configure RADIUS network attributes on the Avaya VPN Gateway. If there is fallback while configuring RADIUS network attributes, you can configure the network attributes similar to the local network attribute configuration. For more information, see “Configuring IP address range and local network attributes” on page 545.

For more information about configuring a RADIUS server, see Chapter 8, “Authentication Methods”.

To retrieve RADIUS network attribute from the RADIUS server, perform the following:

1. **From the System tree view, select VPN Gateways.**

   The VPN Gateway appears.

2. **Select the VPN Gateway name for which you want to enable the RADIUS network attributes.**

   The VPN Summary appears.

3. **Select Authentication.**

   The authentication form appears.

4. **From the authentication server list, select the RADIUS server.**

   The RADIUS authentication form appears.

5. **Click the Network Attributes tab.**

   The Network Attributes form appears.

6. **From the Radius Network Attribute list, select enabled.**

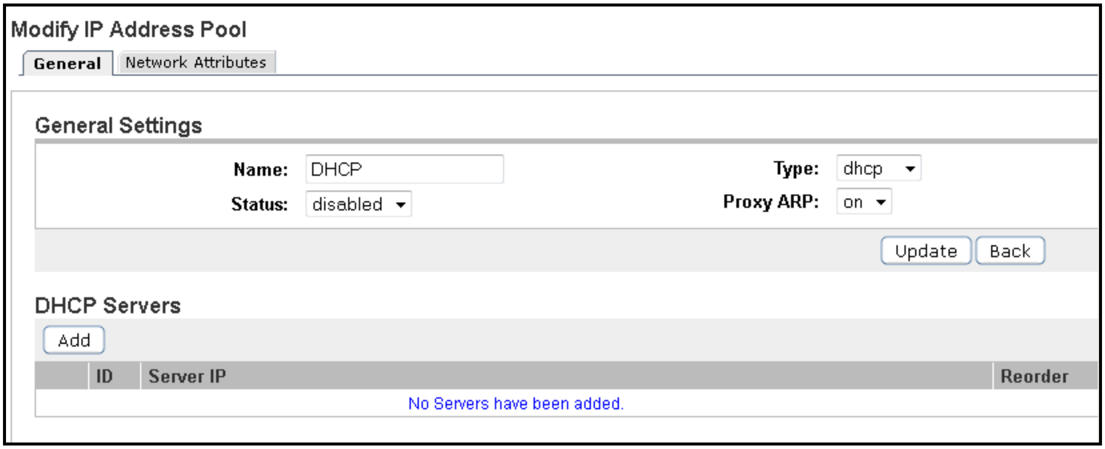
7. **Click Update.**

Configuring DHCP Network Attributes

To configure the pool mechanism for DHCP, perform the following:

1. **Click the General Settings tab.**

   The General Settings form appears.



Modify IP Address Pool

General | Network Attributes

General Settings

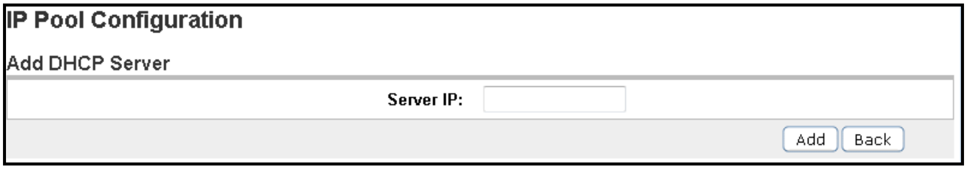
Name:	DHCP	Type:	dhcp
Status:	disabled	Proxy ARP:	on

DHCP Servers

	ID	Server IP	Reorder
No Servers have been added.			

2. **In DHCP Servers, click Add.**

The IP Pool Configuration form appears.



IP Pool Configuration

Add DHCP Server

Server IP:

3. **In the Server IP field, enter the external DHCP server IP address.**
4. **Click Add.**
5. **Click Apply.**

   You can configure network attributes on the Avaya VPN Gateway as fallback values if the DHCP server does not return a specific setting for a network attribute. The configuration is done in the same way as for IP Pools of the `local` type.

   You can associate an Internet Protocol (IP) pool with a particular host in a clustered environment. For more information about creating an Host IP Pool, see "Create Host IP Pool" on page 143.

Creating default IP Pool

Select one configured IP Pool as the default IP Pool. Groups with no IP Pool use the default IP Pool. For more information about creating default IP Pool, see "Create Default IP Pool" on page 615.

Mapping the IP Pool

You can configure several IP Pools with different mechanisms (local, radius, or DHCP). 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 group membership. For more information about mapping the IP Pool, see "Map the IP Pool to User Group (Optional)" on page 616.

Selecting Authentication Order

To set the preferred order in which the defined authentication methods are applied when an user logs on using L2TP tunneling protocol, perform the following steps:

1. **From the System tree view, select VPN Gateways.**

   The VPN Gateways appears.

2. **Select the configured VPN for which you want to set the Authentication Order.**

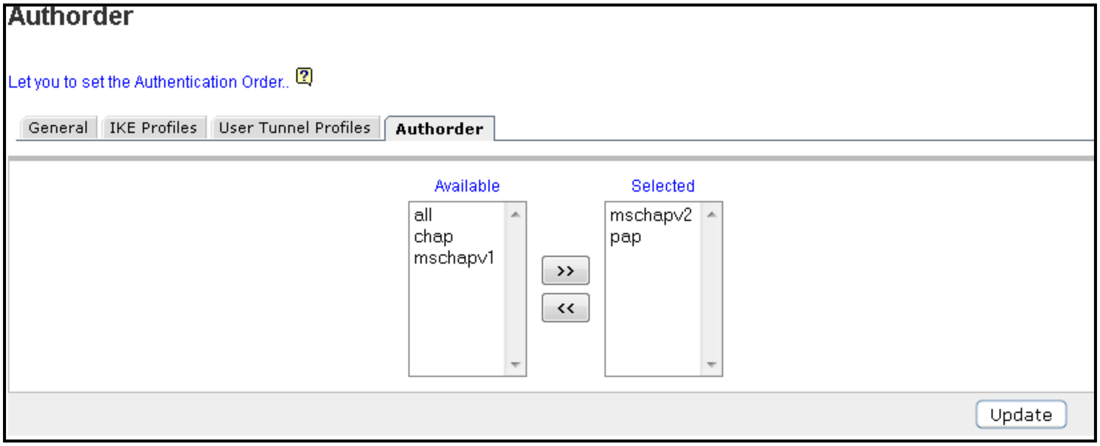
   The VPN Summary screen appears.

3. **Select L2TP.**

   The L2TP settings form appears.

4. **Click the Authentication Order tab.**

   The Authentication Order form appears.



Authorder

Let you to set the Authentication Order..

Available	Selected
all chap mschapv1	mschapv2 pap

NOTE – You must configure MSCHAPv1, CHAP or PAP as primary authentication for L2TP with Apple or Android clients. MS-CHAPv2 does not work for L2TP with Apple and Android clients.

---

5. **From the Available authentication methods, select the required methods.**

6. **Click Update.**

7. **Click Apply.**

Configuring L2TP connection for Windows client

To create a Windows client connection, perform the following procedure:

1. **Select Start, Control panel, Network Connections.**
   The Network Connection window appears.

2. **Click the Create a new connection link.**
   The Welcome to the New Connection Wizard appears.

3. **Click Next.**

4. **Select the Connect to the network at my workplace option, and then click Next.**

5. **Select the Virtual Private Network connection option, and then click Next.**

6. **Enter the name of the connection in Company Name field, and then click Next.**

7. **Enter the host name or IP address of the machine you want to connect to in Host name or IP address field, and then click Next.**

8. **Select the Do not use my smart card option, and then click Next.**

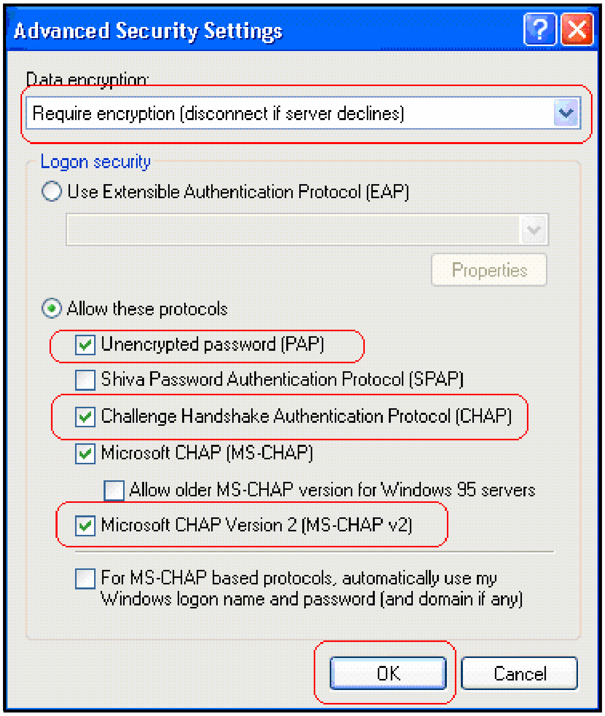
9. **Select the My use only option, and then click Next.**

10. **Select the Add a shortcut to this connection to my desktop checkbox, and then click Finish.**
    The connection is created.

11. **Double click the icon of the newly created connection. The Connect connection dialog box appears.**

12. **Enter the user name and password in the corresponding fields, and click Properties.**
    The Properties dialog box appears.

13. **Open the Security tab, select the Advanced (custom settings) option, and then click Settings. The Advanced Security Settings dialog box appears.**



Data encryption:
Require encryption (disconnect if server declines)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

☑ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP (MS-CHAP)

□ Allow older MS-CHAP version for Windows 95 servers

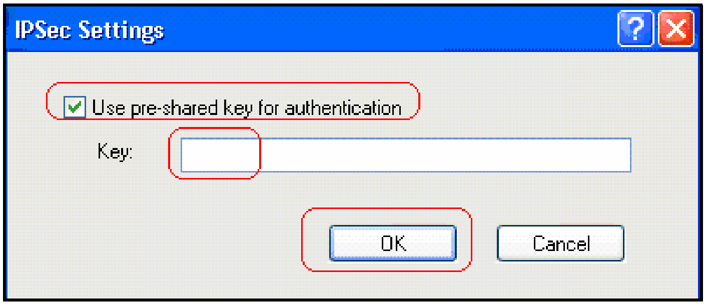
☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

14. **Select the Require encryption from the Data encryption list.**

15. **Select the Allow these protocols option, select the protocols you want to use, and then click OK.**

16. **In the Properties window, click IPSec settings. The IPSec Settings dialog box appears.**



☑ Use pre-shared key for authentication

Key:

17. **Select the Use pre-shared key for authentication checkbox, enter the preshared key in Key field, and then click OK.**

18. **In the Properties window, open the Networking tab.**

19. **Select L2TP IPSec VPN in the Type of VPN list.**

20. **Select Network Monitor Driver, and then click OK.**

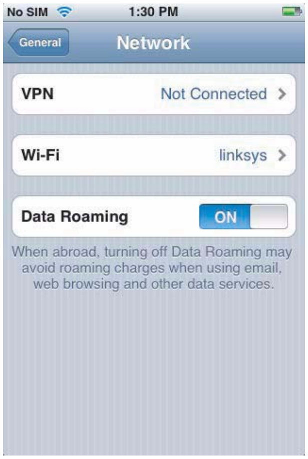
21. **Open the Connect connection window, enter user name and password, and then click Connect.**

Configuring L2TP connection for iPhone client

To create an iPhone client connection, perform the following procedure:

1. **Select Settings, General, Networks from the main menu.**

   The Network setup screen appears.



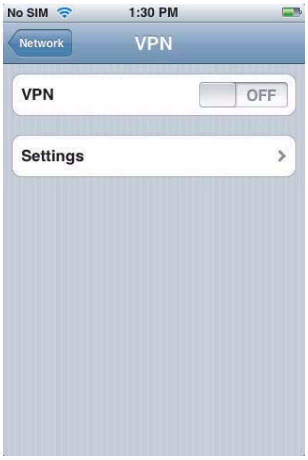
VPN Not Connected

Wi-Fi linksys

Data Roaming ON

When abroad, turning off Data Roaming may avoid roaming charges when using email, web browsing and other data services.

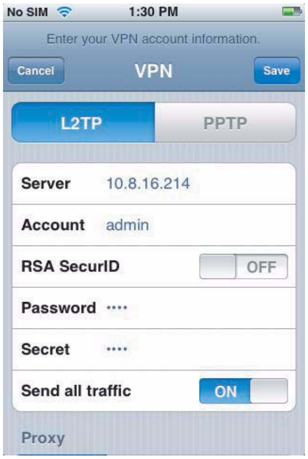
2. **Select VPN. The VPN screen appears.**



VPN OFF

3. **Click Settings, L2TP to configure L2TP connection information.**

   The L2TP configuration screen appears.



Server 10.8.16.214

Account admin

RSA SecurID OFF

Password ••••

Secret ••••

Send all traffic ON

4. **Enter the IP address, user name, password, and PreShared Key (PSK) as defined in your AVG configuration.**

5. **Click Save to save the settings.**

6. **Initiate the VPN connection.**
   After connecting, status information verifies the successful session to the AVG. Now, you can access resources using various applications using the private IP, over an encrypted L2TP connection.

Configuring L2TP connections for Android

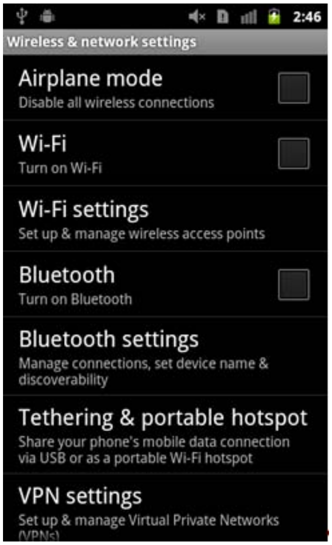
Release 9.0 supports only Android 2.X, 3.X, and 4.X. Use the following procedures when configuring L2TP for Android.

Configuring L2TP connection for Android 3.2 and previous versions

To create an Android client connection, perform the following procedure:

1. **Select Settings, Wireless & Network from the menu.**

   The Wireless & Network settings screen appears.



2:46

Wireless & network settings

Airplane mode □
Disable all wireless connections

Wi-Fi □
Turn on Wi-Fi

Wi-Fi settings
Set up & manage wireless access points

Bluetooth □
Turn on Bluetooth

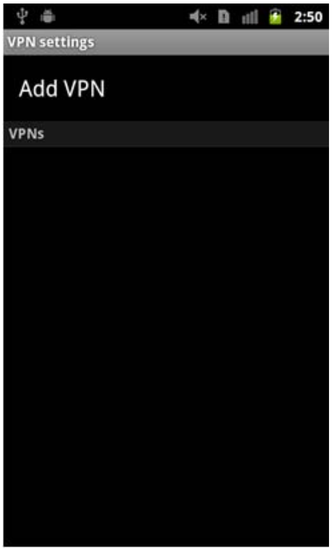
Bluetooth settings
Manage connections, set device name & discoverability

Tethering & portable hotspot
Share your phone's mobile data connection via USB or as a portable Wi-Fi hotspot

VPN settings
Set up & manage Virtual Private Networks (VPNs)

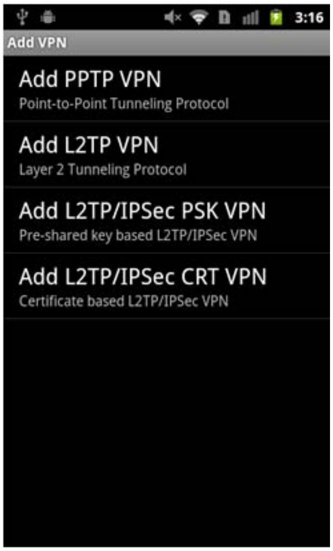
2. **Select VPN Settings.**

   The VPN screen appears.



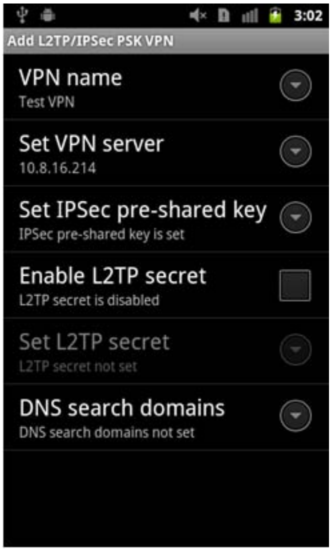
3. **Select Add VPN, Add L2TP/IPSec PSK VPN to configure a pre-shared key based L2TP/IPSec VPN.**

   The L2TP/IPSec PSK VPN configuration screen appears.


3:16
Add VPN
Add PPTP VPN
Point-to-Point Tunneling Protocol
Add L2TP VPN
Layer 2 Tunneling Protocol
Add L2TP/IPSec PSK VPN
Pre-shared key based L2TP/IPSec VPN
Add L2TP/IPSec CRT VPN
Certificate based L2TP/IPSec VPN

4. **Enter a VPN name, IP address and pre-shared key as defined in your AVG configuration.**

   You do not needto use the rest of the options.



Add L2TP/IPSec PSK VPN

VPN name
Test VPN

Set VPN server
10.8.16.214

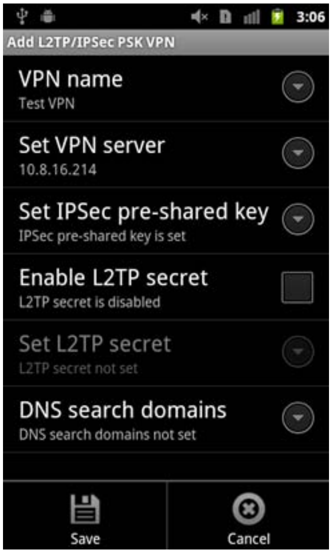
Set IPSec pre-shared key
IPSec pre-shared key is set

Enable L2TP secret □
L2TP secret is disabled

Set L2TP secret
L2TP secret not set

DNS search domains
DNS search domains not set

5. **Click menu and Save to save the settings.**



Add L2TP/IPSec PSK VPN

VPN name
Test VPN

Set VPN server
10.8.16.214

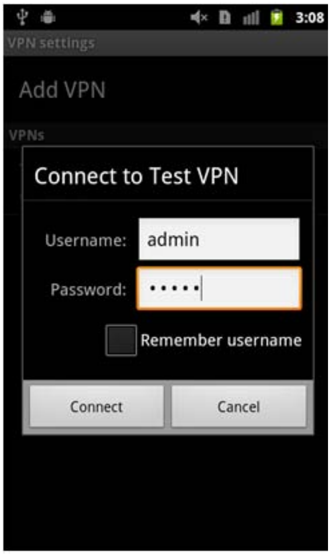
Set IPSec pre-shared key
IPSec pre-shared key is set

Enable L2TP secret □
L2TP secret is disabled

Set L2TP secret
L2TP secret not set

DNS search domains
DNS search domains not set

6. **Initiate the VPN connection by selecting the configured VPN. Enter the user name and password as defined in your AVG configuration and click the Connect button.**



VPN settings

Add VPN

VPNs

Connect to Test VPN

Username: admin

Password: •••••

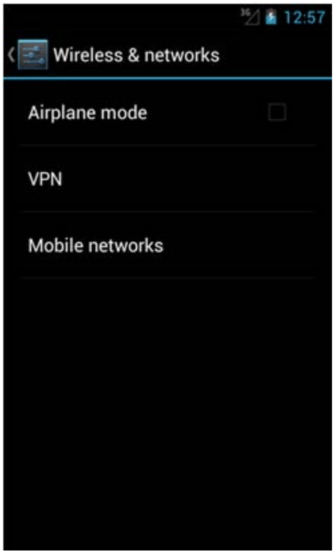
□ Remember username

Configuring L2TP connection for Android 4.0 and higher

To create an Android client connection, perform the following procedure:

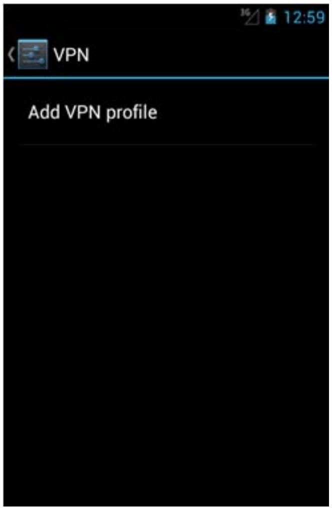
1. **Select Settings, Wireless & networks, More from the menu.**

   The Wireless & Network settings screen appears.



2. **Select VPN menu.**

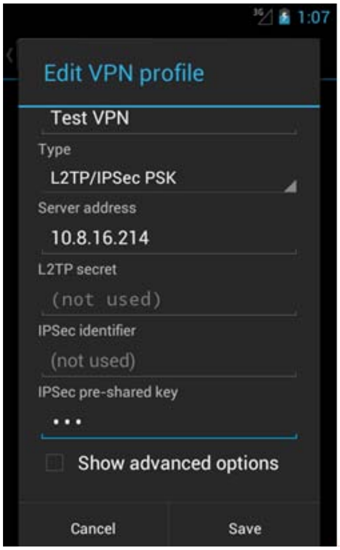
   The VPN screen appears.



3. **Select Add VPN to configure a L2TP/IPSec VPN.**

   The Edit VPN profile configuration screen appears.

4. **Enter a VPN name, IP address and pre-shared key as defined in your AVG configuration. You do not needto use the rest of the options.**



Edit VPN profile

Test VPN

Type

L2TP/IPSec PSK

Server address

10.8.16.214

L2TP secret

(not used)

IPSec identifier

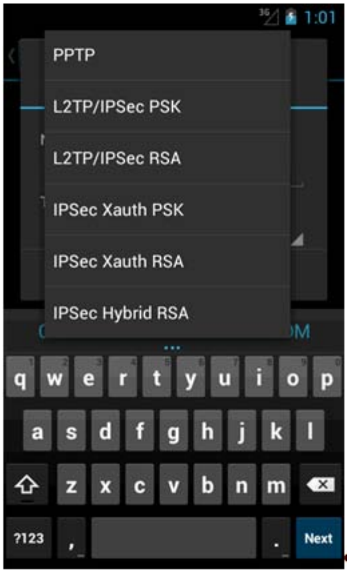
(not used)

IPSec pre-shared key

•••

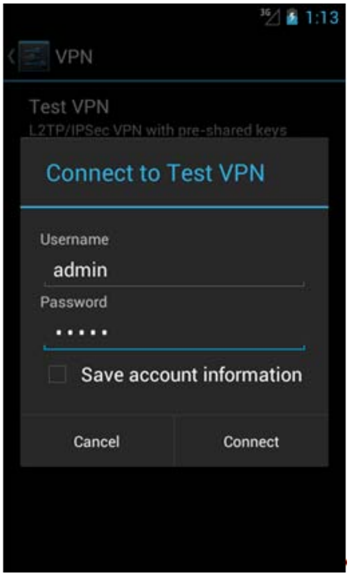
□ Show advanced options

5. **Configure the VPN Type as L2TP/IPSec PSK.**



6. **Click Save to save the settings.**

7. **Initiate the VPN connection by selecting the configured VPN. Enter the user name and password as defined in your AVG configuration and click Connect.**



VPN

Test VPN

L2TP/IPSec VPN with pre-shared keys

Connect to Test VPN

Username

admin

Password

••••••

□ Save account information

CHAPTER 20
Network Access Protection

This chapter provides procedures to configure the Network Access Protection (NAP) for Avaya VPN Gateway device.

Network Access Protection is a Microsoft® technology which enforces system health requirements for clients trying to access private network.

For more information about configuring NAP, see the following:

- "Configuring remote NPS" on page 594
- "Configuring general settings" on page 596
- "Configuring system health validator" on page 598
- "Configuring Windows system health validator" on page 600

Configuring remote NPS

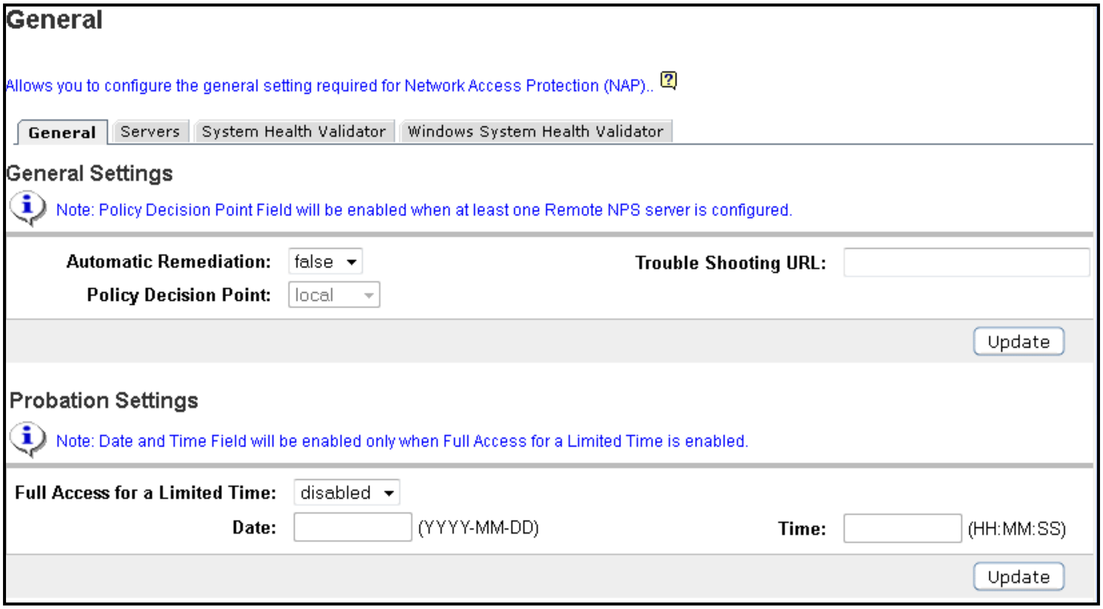
To configure the remote Network Policy Server (NPS), perform the following:

1. **Log on to the BBI as an administrator.**
2. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to enable NAP.**

   The VPN Summary form appears.
4. **Select NAP.**

   The General form appears.



General

Allows you to configure the general setting required for Network Access Protection (NAP)..

General Settings

Note: Policy Decision Point Field will be enabled when at least one Remote NPS server is configured.

Automatic Remediation: false

Trouble Shooting URL:

Policy Decision Point: local

Probation Settings

Note: Date and Time Field will be enabled only when Full Access for a Limited Time is enabled.

Full Access for a Limited Time: disabled

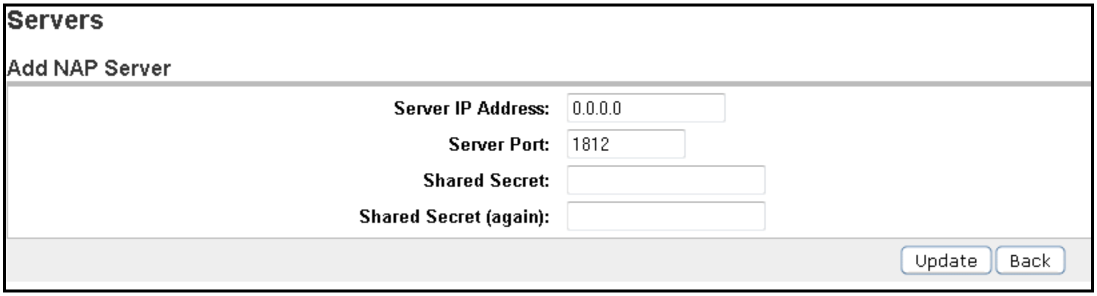
Date: (YYYY-MM-DD)

Time: (HH:MM:SS)

5. **Click the Servers tab.**

6. **Click Add, to add an NPS.**

   The Add NAP Server appears.



Servers

Add NAP Server

Server IP Address: 0.0.0.0

Server Port: 1812

Shared Secret:

Shared Secret (again):

7. **In the Server IP Address field, enter the IP address for the NPS.**

8. **In the Server Port field, enter the Transmission Control Protocol (TCP) port number.**

   The default TCP port is 1812.

9. **In the Shared Secret field, enter the shared secret for the NPS.**

10. **In the Shared Secret (again) field, enter the shared secret to reconfirm.**

11. **Click Update.**

    The NPS server is added to the NAP server list.

    You can move the NPS location ID. For more information, see "Moving the NPS" on page 595.

Moving the NPS

To move the NPS ID, perform the following in the server form:

1. **From the Move Server from list, select the server location ID from where the server needs to be moved.**

2. **From the Move Server from to list, select the server location ID to which the server needs to be moved.**

3. **Click Move, to move the server location.**

   The server list is updated.

Configuring general settings

To configure NAP general settings, perform the following:

1. **Log on to the BBI as an administrator user.**
2. **From the System tree view, select VPN Gateways.**

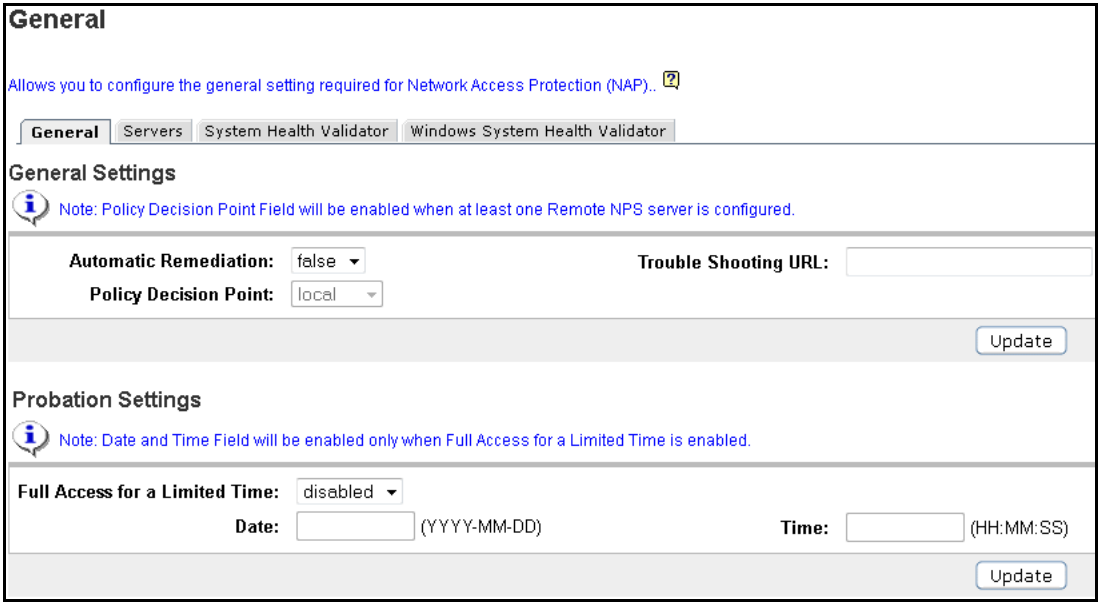
   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to enable NAP.**

   The VPN Summary form appears.
4. **Select NAP.**

   The NAP general form appears.

5. **Click the General tab.**

   The general form appears.



General

Allows you to configure the general setting required for Network Access Protection (NAP)..

General Settings

Note: Policy Decision Point Field will be enabled when at least one Remote NPS server is configured.

Automatic Remediation: false

Policy Decision Point: local

Trouble Shooting URL:

Probation Settings

Note: Date and Time Field will be enabled only when Full Access for a Limited Time is enabled.

Full Access for a Limited Time: disabled

Date: (YYYY-MM-DD)

Time: (HH:MM:SS)

6. **From the Automatic Remediation list, select true.**

7. **From the Policy Decision Point list, select local or remote.**

   The Policy Decision Point is enabled only when the remote NPS is configured.

8. **In the Troubleshooting URL field, enter the URL name for patch updates.**

9. **Click Update.**

10. **From the Full Access for a Limited Time list, select enabled.**

11. **In the Date field, enter the date to start limited access.**

12. **In the Time field, enter the time to start limited access.**

13. **Click Update.**

Configuring system health validator

System health validator (SHV) validates the Statement of Health (SoH) submitted by a SHA complies with the required health state. System health validator run on the NPS server and must coordinate with the output from all of the SHVs. To configure an SHV, perform the following steps:

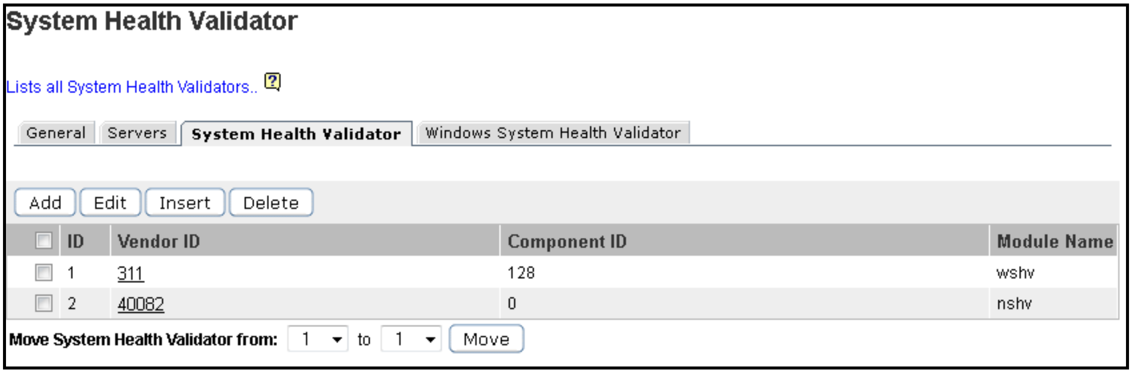
1. **Log on to the BBI as an administrator user.**
2. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to enable NAP.**

   The VPN Summary form appears.
4. **Select NAP.**

   The NAP General form appears.
5. **Click the System Health Validator tab.**

   The system health validator form appears.



System Health Validator

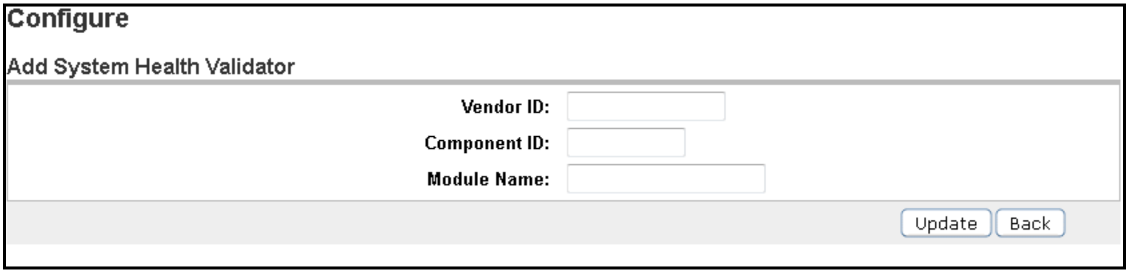
Lists all System Health Validators..

□	ID	Vendor ID	Component ID	Module Name
□	1	311	128	wshv
□	2	40082	0	nshv

Move System Health Validator from: 1 to 1

6. **Select Add, to add an SHV.**

   The Add System Health Validator form appears.



Configure

Add System Health Validator

Vendor ID:	
Component ID:	
Module Name:	

7. **In the Vendor ID field, enter the vendor ID.**
8. **In the Component ID field, enter the component ID.**
9. **In the Module Name field, enter the module name.**
10. **Click Update.**

    The SHV is added to the list.

    You can move the SHV location ID. For more information, see "Moving the SHV ID" on page 599.

Moving the SHV ID

To move the SHV ID, perform the following in the System Health Validator form:

1. **From the Move System Health Validation from list, select the validator ID to move the validator.**
2. **From the Move System Health Validation from list, select the validator ID to move the validator.**
3. **Click Move, to move the validator.**

   The SHV list is updated.

Configuring Windows system health validator

To configure Windows system health validator, perform the following:

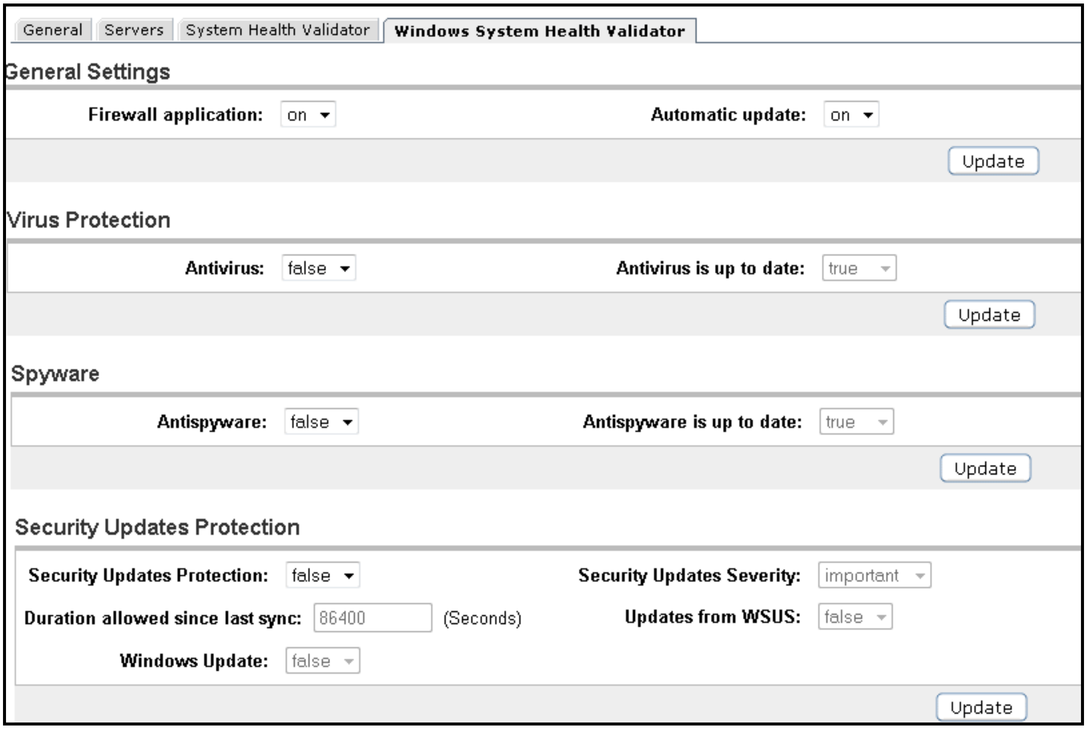
1. **Log on to the BBI as an administrator user.**
2. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to enable NAP.**

   The VPN Summary form appears.
4. **Select NAP.**

   The General form appears.
5. **Click the Windows System Health Validator tab.**

   The Windows system health validator form appears.



General Settings

Firewall application: on
Automatic update: on

Virus Protection

Antivirus: false
Antivirus is up to date: true

Spyware

Antispyware: false
Antispyware is up to date: true

Security Updates Protection

Security Updates Protection: false
Security Updates Severity: important
Duration allowed since last sync: 86400 (Seconds)
Updates from WSUS: false
Windows Update: false

To configure different Windows SHV, perform the following:

- "Enabling firewall" on page 601
- "Enabling virus protection" on page 601
- "Enabling antispyware" on page 601
- "Enabling security updates protection" on page 601

Enabling firewall

To enable the firewall, perform the following in General Settings:

1. **From the Firewall application list, select on.**

   The Automatic updates option is enabled for selection.

2. **From the Automatic updates list, select on.**
3. **Click Update.**

Enabling virus protection

To enable the virus protection, perform the following steps:

1. **From the Virus Protection list, select true.**

   The Antivirus is update is up to date option is enabled for selection.

2. **From the Antivirus is update is up to date list, select true.**
3. **Click Update.**

Enabling antispyware

To enable antispyware, perform the following steps:

1. **From the Antispyware list, select true.**

   The Antispyware is up to date option is enabled for selection.

2. **From the Antispyware is up to date list, select true.**
3. **Click Update.**

Enabling security updates protection

To enable security updates protection, perform the following steps:

1. **From the Security Updates Protection list, select true.**

The other options are enabled for selection.

2. **In the Duration allowed since last sync field, enter the duration.**

   Mention the duration allowed in seconds. The duration is from be between 3600 and 394200.

3. **From the Windows Update list, select true to enable updates from Windows.**

4. **From the Security Updates Severity list, select severity.**

5. **From the WSUS list, select true to enable Windows Server Update Service (WSUS).**

6. **Click Update.**

7. **Click Apply.**

CHAPTER 21
Transparent Mode

This chapter describes how to configure the Avaya VPN Gateway for use with the Avaya VPN Client.

NOTE – In AVG 8.x and 9.0, the SSL Client mechanism is not supported for transparent mode. AVG 8.x and 9.0 support Avaya VPN Client (SSL) and Avaya VPN Client (IPsec) mechanisms for full transparent access.

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.

The transparent mode requires the user to install the Avaya VPN Client. The Avaya VPN Gateway will then act as the 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.

Before you start configuring the Avaya VPN Gateway cluster, you should have performed the initial setup procedure (see the "Initial Setup" chapter in the *User's Guide*).

Configuring Avaya VPN Client (IPsec)

For users with the Avaya VPN Client installed, access to intranet resources can be made available through the Avaya VPN Gateway through a secure IPsec connection.

Server Configuration

To enable use of the Avaya VPN Client in IPSec mode, follow the basic instructions for setting up a VPN in Chapter 5, “Clientless Mode”. The same configuration applies to both clientless and transparent mode. Then continue with the following steps.

NOTE – User name and password authentication is only supported if the user exists in the Avaya VPN Gateway’s local database.

Enable IPsec

IPsec support is disabled by default on the Avaya VPN Gateway.

1. **In the System tree view, select VPN Gateways.**

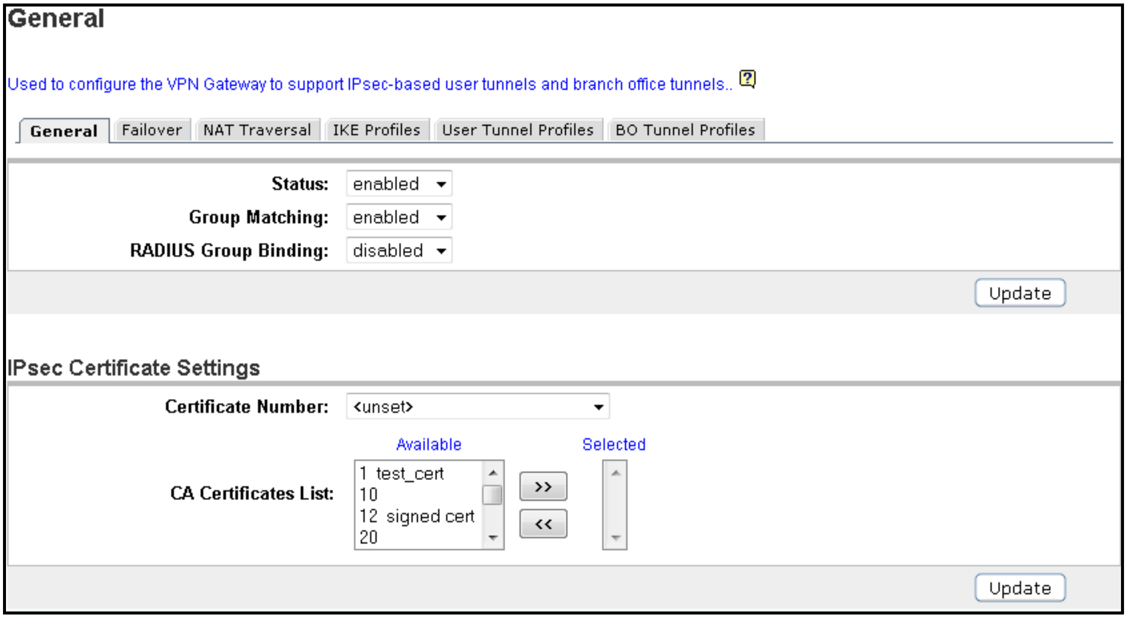
   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name.**

   VPN Summary screen appears.

3. **Under Settings, select IPSec.**

4. **Select General.**
   General screen is displayed.



General

Used to configure the VPN Gateway to support IPsec-based user tunnels and branch office tunnels..

Status: enabled

Group Matching: enabled

RADIUS Group Binding: disabled

IPsec Certificate Settings

Certificate Number: <unset>

CA Certificates List:

Available	Selected
1 test_cert 10 12 signed cert 20	

5. **In the Status list box, select `enabled`.**

   This step enables IPsec tunnel encryption mode. Transport mode is not supported by the Avaya VPN Gateway software.

6. **Click Update.**

7. **If client certificates are used for VPN client authentication, reference the server certificate in the Certificate Number list box.**

   The server certificate must be stored on the Avaya VPN Gateway. For detailed information about certificate management, see the “Certificates and Client Authentication” chapter in the *User’s Guide*.

8. **If client certificates are used for client authentication, reference the CA certificate(s) used to sign the client certificate(s) by moving it to the Selected box.**

   The CA certificate must be stored on the Avaya VPN Gateway. For detailed information about certificate management, see the “Certificates and Client Authentication” chapter in the *User’s Guide*.

   The server certificate must be signed by a CA certificate that is a trusted CA certificate on the client machine.

9. **Click Update.**

Create an IKE Profile

This step creates an IKE profile. The default settings for the IKE profile are usually fine for use with the Avaya VPN Client. If needed, several different IKE profiles can be created with different settings for encryption, NAT traversal and so on. For detailed information about available settings, see the *User's Guide*.

1. **In the System tree view, select VPN Gateways**

   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name.**

   VPN Summary screen appears.

3. **Under Settings, select IP Sec.**

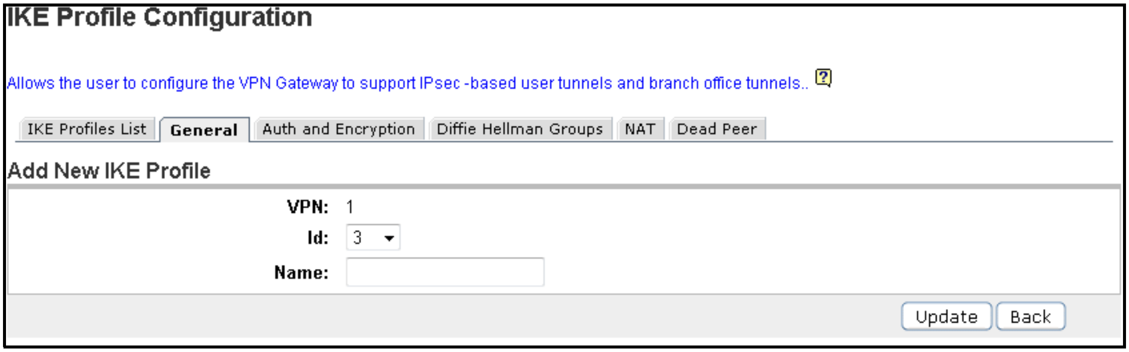
   General screen is displayed.

4. **Click on IKE Profiles tab.**

   IKE Profiles screen is displayed.

5. **Click Add.**

   The Add New IKE Profile form is displayed.



IKE Profile Configuration

Allows the user to configure the VPN Gateway to support IPsec -based user tunnels and branch office tunnels..

Add New IKE Profile

VPN:	1
Id:	3
Name:	

6. **Click Update.**

   The IKE Profiles form is redisplayed with the new IKE profile.

Create a User Tunnel Profile

Use this procedure to create a user tunnel profile. The user tunnel defines different criteria for the IPsec user 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 Avaya VPN Client. For detailed information about available settings, see the *User's Guide*.

1. **In the System tree view, select VPN Gateways**

   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name**

   VPN Summary screen appears.

3. **Under Settings, select IP Sec**

   General screen is displayed.

4. **Click on the User Tunnel Profiles tab.**

   The User Tunnel Profiles screen is displayed.

5. **Click Add.**

   The Add New User Tunnel Profile form is displayed.

6. **In the Name field, enter a name for the user tunnel profile.**

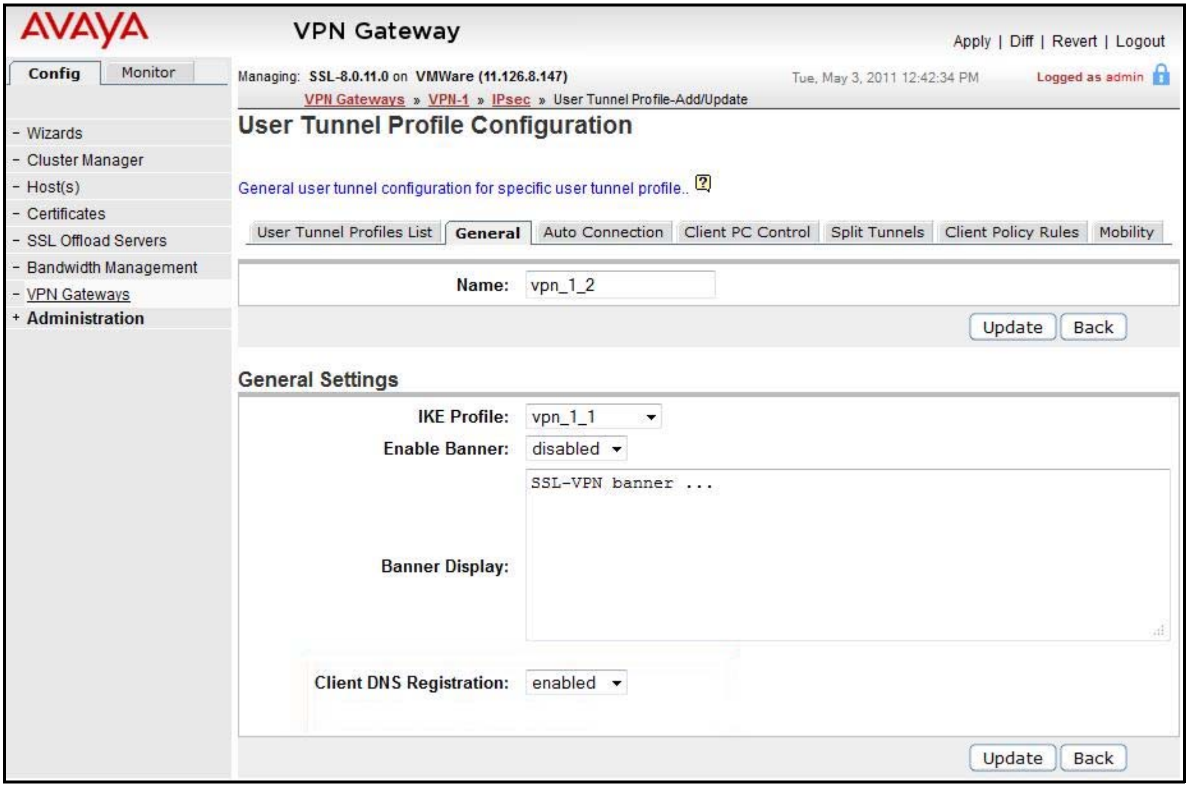
7. **Click Update.**

   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 is displayed.

9. **In the IKE profile list box, select the IKE profile name we created in the previous section.**



Managing: SSL-8.0.11.0 on VMWare (11.126.8.147)

Tue, May 3, 2011 12:42:34 PM

User Tunnel Profile Configuration

General user tunnel configuration for specific user tunnel profile..

Name: vpn_1_2

General Settings

IKE Profile: vpn_1_1

Enable Banner: disabled

Banner Display: SSL-VPN banner ...

Client DNS Registration: enabled

10. **In the Enable Banner list box, select whether or not a banner should be displayed in the Avaya 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 Avaya VPN Client upon login.

11. **Select the DNS registration scheme from the Client DNS Registration field drop-down menu.**

    - `Enabled` means that the AVC registers each time it connects to the VPN.
    - `Disabled` means that the AVC does not register.

12. **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 Avaya VPN Gateway.

If you have not yet configured user groups, you can follow the following steps once the desired groups have been configured. Group configuration is described in Chapter 8, “Groups, Access Rules and Profiles”.

1. **In the System tree view, select VPN Gateways**

   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name**

   VPN Summary screen appears.

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

   Group screen is displayed.

4. **Click Add.**

   Add a Group screen is displayed.

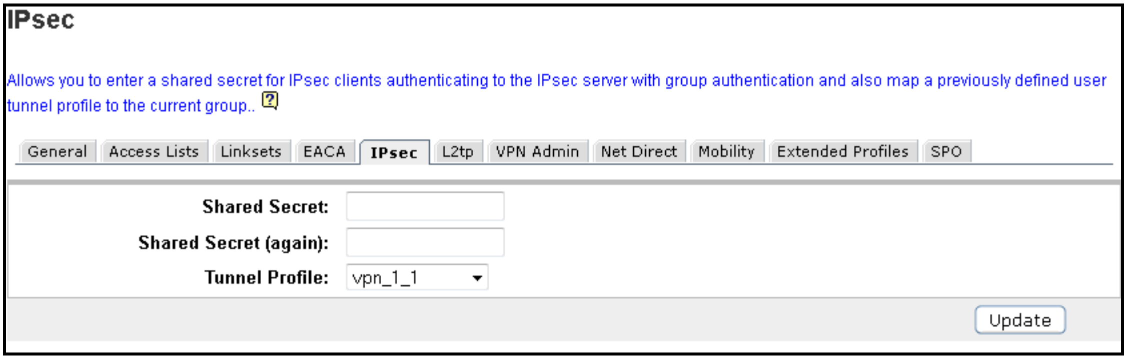
5. **In the Name field, enter a name for group.**

6. **Click Update.**

   Modify a group screen is displayed.

7. **Click on IPsec tab.**

   The IPsec form is displayed.



IPsec

Allows you to enter a shared secret for IPsec clients authenticating to the IPsec server with group authentication and also map a previously defined user tunnel profile to the current group..

Shared Secret:

Shared Secret (again):

Tunnel Profile: vpn_1_1

8. **In the Shared secret field, enter the group secret (used for group authentication).**

   The group password entered by the remote user in the Avaya VPN Client should match the group secret configured here.

9. **Confirm the shared secret in the field.**

10. **In the Tunnel Profile list, select the desired profile.**

11. **Click update.**

Create IP Pool

The IP Pool comes into play when the remote user tries to access a host using the Avaya VPN Client. A new IP address has to be assigned as source IP for the unencrypted connection between the Avaya 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 Avaya VPN Client (SSL) access as well (see Chapter 7, “Net Direct”). If you have already configured an IP Pool for use with the Avaya VPN Client (SSL) client, this Pool can also be used for the Avaya VPN Client.

1. **In the System tree view, select VPN Gateways.**

   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name**

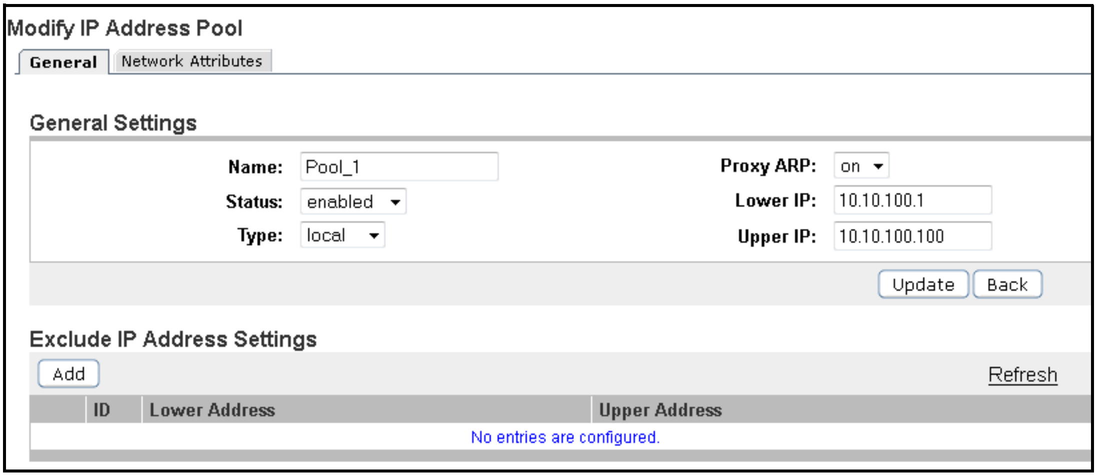
   VPN Summary screen appears.

3. **Under Settings, select IP Pool.**

   IP Pool form is displayed.

4. **Under IP Pool list, click Add.**

   IP Pool Configuration form is displayed. The first available IP Pool number is suggested in the IP Pool ID list box.



Modify IP Address Pool

General Settings

Name:	Pool_1	Proxy ARP:	on
Status:	enabled	Lower IP:	10.10.100.1
Type:	local	Upper IP:	10.10.100.100

Exclude IP Address Settings

ID	Lower Address	Upper Address
No entries are configured.		

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. **From the Type list, select the local, radius, or DHCP network attribute.**

   You can assign the network attributes (including IP address) either locally (from the Avaya VPN Gateway) from an external RADIUS server, or from an external DHCP server.

   For IP Pools of the `local` type, you must configure the network attributes on the Avaya VPN Gateway. For IP Pools of the `radius` and `dhcp` types, you can configure network attributes on the Avaya VPN Gateway as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute.

8. **In Proxy ARP list, select any one of the following:**

   yes, to enable the IP address for a specific client connection and respond to ARP requests on behalf of the L2TP VPN client for return traffic

   Or

   no, to disable the return traffic to reach its destination unless specific routes are configured

   Or

   all, to enable the IP address for a specific client connection without proxy ARP on all interfaces

9. **Click Update.**

   The IP Pool Configuration displays different entry forms depending on the selected IP Pool mechanism (`local`, `radius` or `dhcp`). Use the following steps according to your IP Pool configuration selection:

10. **In the Lower IP field, enter the lower limit to include in the IP range.**
11. **In the Upper IP field, enter the upper limit to include in the IP range.**
12. **In the Exclude IP Settings, click Add.**

    The Add Exclude IP Address Range form appears.

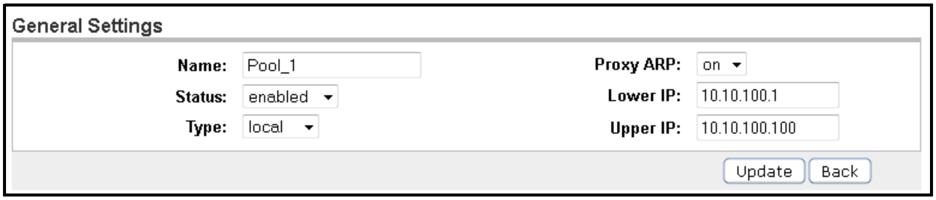
13. **In the Lower IP Limit field, enter the lower limit to exclude from IP range.**
14. **In the Upper IP Limit field, enter the upper limit to exclude from IP range.**
15. **Click Update.**

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism to `local` (as described in Step 7 in the previous section), you should configure the desired IP address range. You can also configure network attributes to be retrieved from the Avaya VPN Gateway 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.

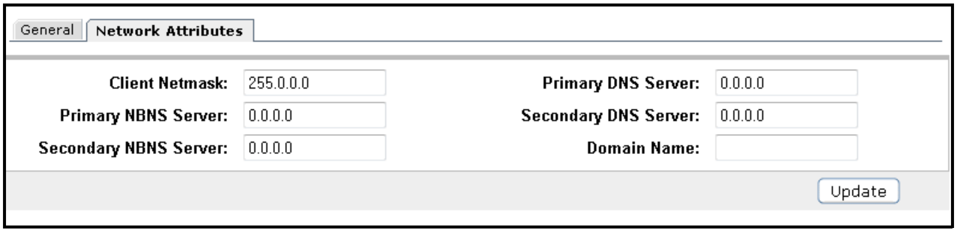
1. **In the Lower IP and Upper IP fields, configure an IP address range.**



General Settings

Name:	Pool_1	Proxy ARP:	on
Status:	enabled	Lower IP:	10.10.100.1
Type:	local	Upper IP:	10.10.100.100

2. **Scroll down to Network Attributes Settings and configure the desired network attributes settings (optional).**



Client Netmask:	255.0.0.0	Primary DNS Server:	0.0.0.0
Primary NBNS Server:	0.0.0.0	Secondary DNS Server:	0.0.0.0
Secondary NBNS Server:	0.0.0.0	Domain Name:	

The Avaya 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 Step 1. 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 Avaya 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 Avaya 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>VPN #>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 pool mechanism to `radius` (as described in the section “Create IP Pool” on page 610), you should configure the Avaya VPN Gateway to retrieve network attributes from a RADIUS server.

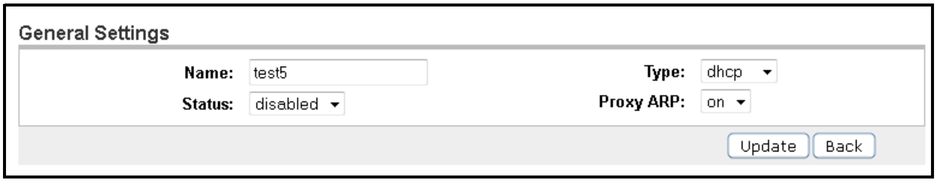
How to configure a RADIUS server is described in Chapter 9, “Authentication Methods”.

To configure the Avaya VPN Gateway to retrieve network settings (including client IP address) through RADIUS attributes from an external RADIUS server, go to VPN Gateways>VPN #>Authentication>RADIUS>Network Attributes. 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 Avaya VPN Gateway 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 613 for instructions).

Configure DHCP Network Attributes

If you set the pool mechanism to `dhcp` (as described in the section “Create IP Pool” on page 610), you should configure the Avaya VPN Gateway to retrieve network attributes from a DHCP server.

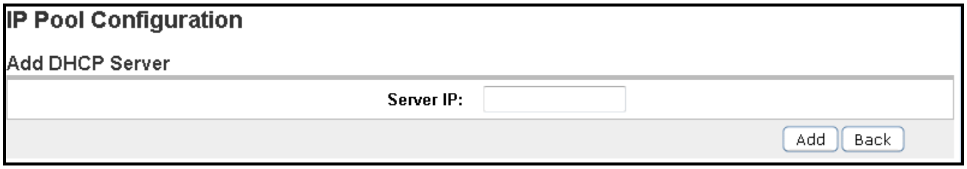


General Settings

Name:	test5	Type:	dhcp
Status:	disabled	Proxy ARP:	on

1. **Under DHCP Servers, click Add.**

2. **Configure the external DHCP server IP address.**



IP Pool Configuration

Add DHCP Server

Server IP:

3. **Click Add.**

4. **Apply the changes.**

   Network attributes can also be configured on the Avaya VPN Gateway 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 613 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.**

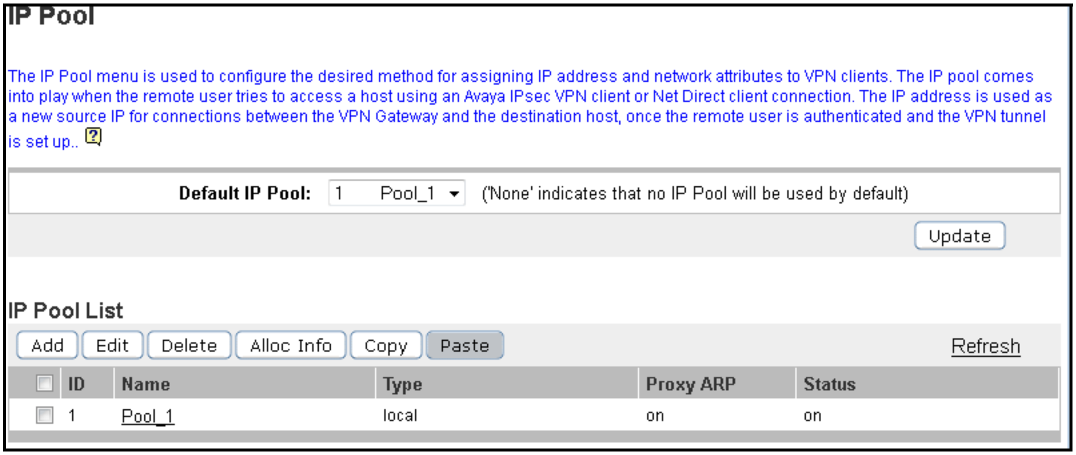
   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name**

   VPN Summary screen appears.

3. **Under Settings, select IP Pool.**

IP Pool form is displayed.



IP Pool

The IP Pool menu is used to configure the desired method for assigning IP address and network attributes to VPN clients. The IP pool comes into play when the remote user tries to access a host using an Avaya IPsec VPN client or Net Direct client connection. The IP address is used as a new source IP for connections between the VPN Gateway and the destination host, once the remote user is authenticated and the VPN tunnel is set up..

Default IP Pool: 1 Pool_1 ('None' indicates that no IP Pool will be used by default)

IP Pool List

□	ID	Name	Type	Proxy ARP	Status
□	1	Pool_1	local	on	on

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 page 610, 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.

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. 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.**

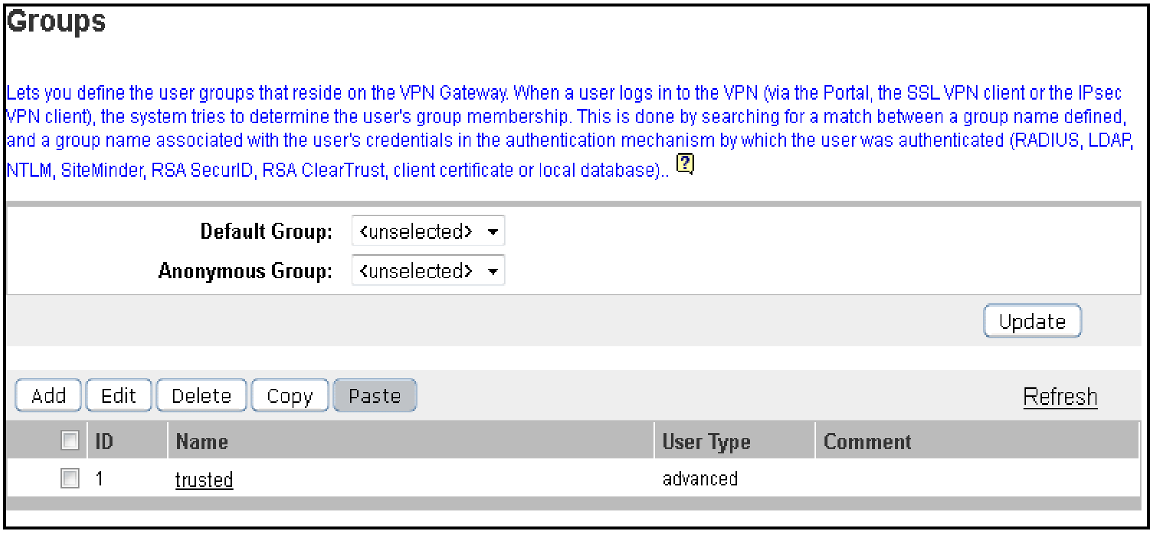
   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name.**

   VPN Summary screen appears.

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

The Groups form is displayed.



Groups

Lets you define the user groups that reside on the VPN Gateway. When a user logs in to the VPN (via the Portal, the SSL VPN client or the IPsec VPN client), the system tries to determine the user's group membership. This is done by searching for a match between a group name defined, and a group name associated with the user's credentials in the authentication mechanism by which the user was authenticated (RADIUS, LDAP, NTLM, SiteMinder, RSA SecurID, RSA ClearTrust, client certificate or local database)..

Default Group: <unselected>

Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

4. **Select the check box next to the group to which you want to map an IP Pool.**

5. **Click Edit**

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.**

Enable Full Access Tab

If not already active, the Avaya 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 an Avaya VPN Router (in `contivity` IPsec mode) or to the Avaya 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 Avaya VPN Client from the **Full Access** page, see Chapter 6, "The Portal from an End-User Perspective".

1. **In the System tree view, select VPN Gateways.**

   VPN Gateways screen is displayed.

2. **Select the VPN Gateway name.**

   VPN Summary screen appears.

3. **Under Settings, select Portal.**

   The Portal General Settings screen is displayed.

4. **Click on the Full Access tab.**

   The Portal Full Access screen is displayed.

5. **In the Status list box, select enabled.**

6. **In the IPsec mode list box, select the desired IPsec mode.**

   This step lets you select the desired IPsec mode for the Avaya VPN Client, that is, whether the client should connect to an existing Avaya VPN Router (formerly Contivity) or the VPN Gateway.

   - contivity: Instructs the Avaya VPN Client to connect to a VPN Router. Proceed to Step 8 to configure VPN Router access.
   - native: Instructs the client to connect to the VPN Gateway.

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

   Configuration is complete.

   To complete the configuration when contivity mode is selected, enter the desired VPN Router IP address in the Contivity IP field.

8. **For group authentication to the VPN Router, enter the desired group ID in the Contivity Group ID field.**

9. **In the Contivity Group Password field, enter the shared secret used for group authentication.**

10. **Enter the shared secret again to confirm.**

11. **Click Update.**

12. **Apply the changes.**

Client Configuration

The Avaya VPN Client can authenticate to the Avaya VPN Gateway in three ways:

- Group authentication
- User name and password authentication
- Client certificate authentication

Group Authentication

1. **Create a new profile on the Avaya 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 604.**

6. **Under Group Authentication Options, verify that Group Password Authentication is selected.**

7. **Click OK.**

8. **Click Save.**

Configuring Avaya VPN Client (SSL)

Configuring the SSL Avaya VPN Client is similar to that of configuring Avaya VPN Client (SSL). Complete the following procedures when configuring the Avaya VPN Client (SSL).

Server Configuration

To enable usage of the Avaya VPN Client (SSL) client, follow the basic instructions in Chapter 5, "Clientless Mode" on how to set up a VPN. Once completed, continue with the instructions in the following sections.

Create IP Pool

The IP Pool comes into play when the remote user tries to access a host using Avaya VPN Client (SSL). A new IP address has to be assigned as source IP for the unencrypted connection between the Avaya VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

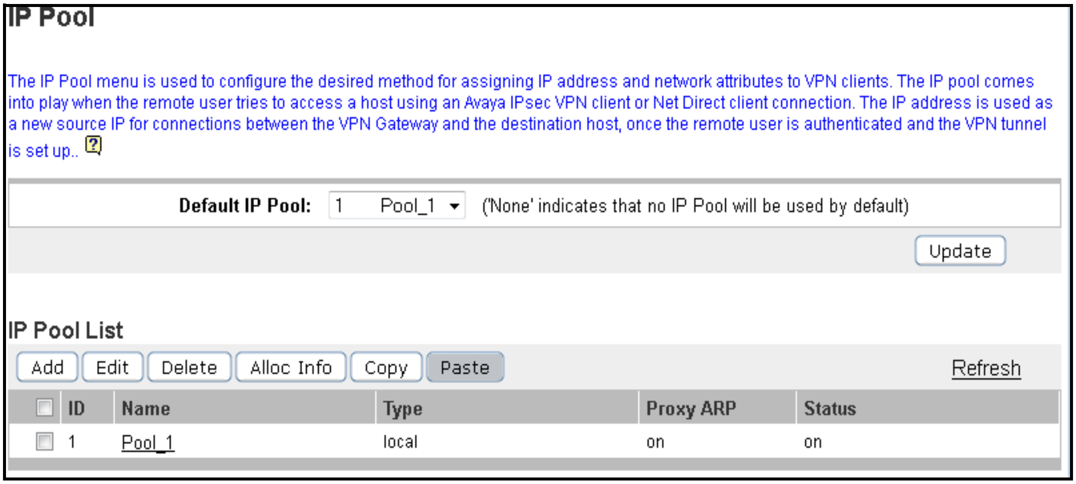
Several IP Pools can be configured, each with a unique ID number and unique properties. By mapping the desired IP Pool to a user group, you can create different methods for IP address and network attributes assignment for different user groups.

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 VPN Client) as well (see "Configuring Avaya VPN Client (IPsec)" on page 604"). If you have already configured an IP Pool for use with the Avaya VPN Client, this pool can also be used for the Avaya VPN Client (SSL) client.

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on IP Pool settings.**

The IP Pool form is displayed.



IP Pool

The IP Pool menu is used to configure the desired method for assigning IP address and network attributes to VPN clients. The IP pool comes into play when the remote user tries to access a host using an Avaya IPsec VPN client or Net Direct client connection. The IP address is used as a new source IP for connections between the VPN Gateway and the destination host, once the remote user is authenticated and the VPN tunnel is set up..

Default IP Pool: 1 Pool_1 ▾ ('None' indicates that no IP Pool will be used by default)

IP Pool List

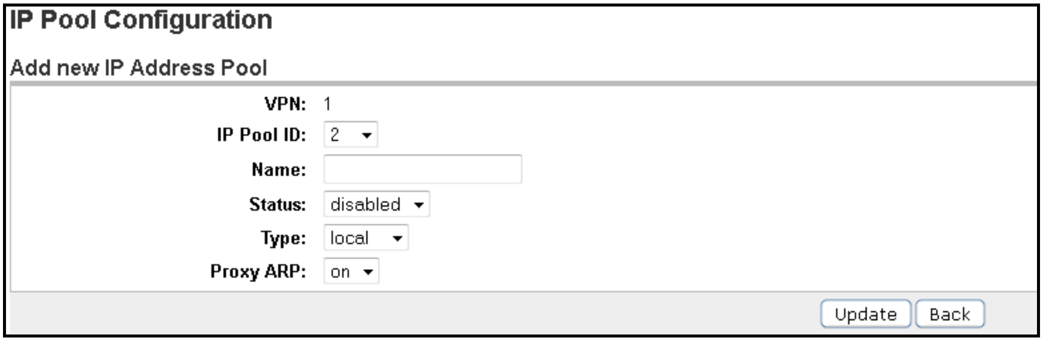
□	ID	Name	Type	Proxy ARP	Status
□	1	Pool_1	local	on	on

5. **Specify a previously created IP Pool number.**
   This IP Pool will be the default IP Pool for the VPN, that is its settings will be used when no IP Pool is specified for a specific user group in the VPN. The IP Pool governs how IP addresses and network attributes are assigned to IPsec client connections and Avaya VPN Client (SSL) client connections.

6. **Gives the user the ability to set the number of IP Pools for each VPN.**
   By default the number of IP Pools for each VPN is set as 30. In order to increase the number of IP Pools for a given VPN beyond 30, this value needs to be set. But the total number of IP Pools across all VPNs can only be 1024.

7. **Under IP Pool List, click Add.**

   The IP Pool Configuration form is displayed.



IP Pool Configuration

Add new IP Address Pool

VPN:	1
IP Pool ID:	2 ▾
Name:	
Status:	disabled ▾
Type:	local ▾
Proxy ARP:	on ▾

The first available IP Pool number is suggested in the IP Pool ID list box.

8. **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.

9. **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.

10. **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 (from the Avaya VPN Gateway), from an external RADIUS server or from an external DHCP server.

    For IP Pools of the `local` type, network attributes should be configured on the Avaya VPN Gateway (see next section). For IP Pools of the `radius` and `dhcp` types, network attributes can be configured on the Avaya VPN Gateway as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute.

11. **If needed, change the default proxy ARP setting.**

    `on`: Means that the Avaya VPN Gateway that handed out the IP address for a specific client connection will respond to ARP requests on behalf of the Avaya VPN Client (SSL) client for return traffic. The Avaya 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.

12. **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 following description depending on your choice.

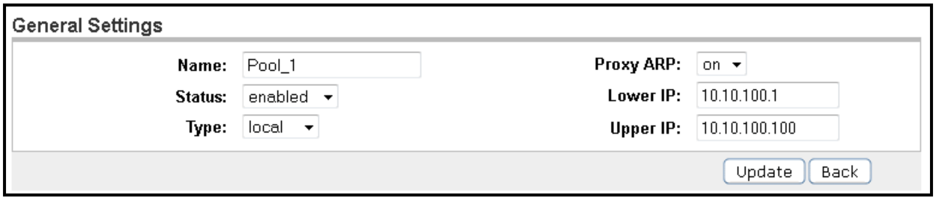
    You can associate an Internet Protocol (IP) Pool with a particular host in a clustered environment. For more information about creating an Host IP Pool, see "Create Host IP Pool" on page 626.

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism to `local` (as described in Step 7 in the previous section), you should configure the desired IP address range. You can also configure network attributes to be retrieved from the Avaya VPN Gateway 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.**



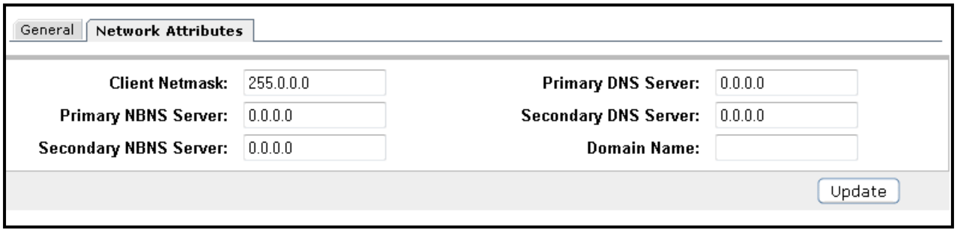
General Settings

Name: Pool_1
Status: enabled
Type: local
Proxy ARP: on
Lower IP: 10.10.100.1
Upper IP: 10.10.100.100

2. **Click Update.**

3. **Scroll down to Exclude IP Address Settings, click Add to specify IP addresses that you wish to exclude, and then click Update (optional).**

4. **Click the Network Attributes tab, and configure the desired network attributes settings in Network Attribute Settings (optional).**



Client Netmask: 255.0.0.0
Primary NBNS Server: 0.0.0.0
Secondary NBNS Server: 0.0.0.0
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0
Domain Name:

The Avaya VPN Client (SSL) 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 Step 1. 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 Avaya VPN Client (SSL) 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 Avaya VPN Client (SSL) 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>VPN #>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 Avaya VPN Client (SSL) 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.

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

Configure RADIUS Settings

If you set the pool mechanism to `radius` (as described in the section "Create IP Pool" on page 610), you should configure the Avaya VPN Gateway to retrieve network attributes from a RADIUS server.

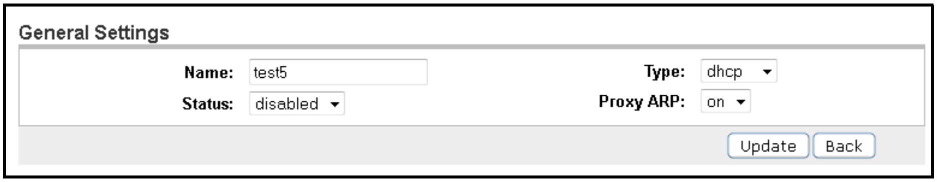
How to configure a RADIUS server is described in Chapter 9, "Authentication Methods".

To configure the Avaya VPN Gateway to retrieve network settings (including client IP address) through RADIUS attributes from an external RADIUS server, go to VPN Gateways>VPN #>Authentication>RADIUS>Network Attributes. 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 etc.

Network attributes can also be configured on the Avaya VPN Gateway 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 4 on page 623 for instructions).

Configure DHCP Settings

If you set the pool mechanism to `dhcp` (as described in the section "Create IP Pool" on page 610), you should configure the Avaya VPN Gateway to retrieve client IP address and network attributes from a DHCP server.

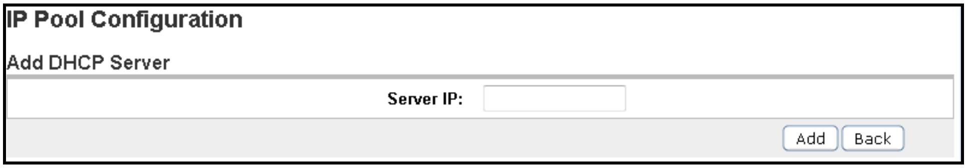


General Settings

Name:	test5	Type:	dhcp
Status:	disabled	Proxy ARP:	on

1. **Under DHCP Servers, click Add.**

2. **Configure the external DHCP server IP address.**



IP Pool Configuration

Add DHCP Server

Server IP:

3. **Click Add.**

4. **Apply the changes.**

   Network attributes can also be configured on the Avaya VPN Gateway 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 4 on page 623 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. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on IP Pool.**

   IP Pool form appears.

5. **In the Default IP Pool list box, select an existing IP Pool as the default IP Pool.**

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

Create Host IP Pool

You can associate an IP Pool with a particular host in a clustered environment. Due to this association, the router on the private side of the cluster knows which interface is associated with each IP address allocated to the end user to send the packets back to the end user during the next hop. The interfaces supported are Net Direct (ND), Net Direct Installable Client (NDIC), Avaya VPN Client, and L2TP/IPsec.

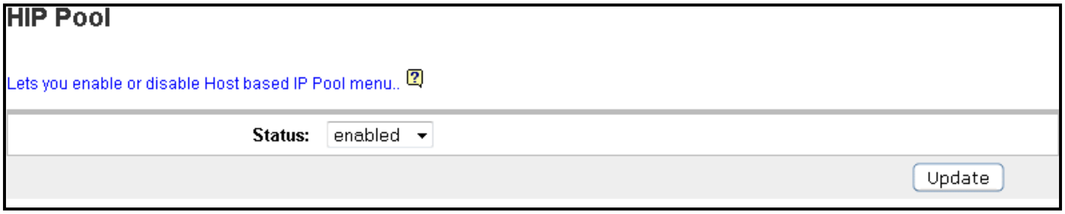
To create the Host IP Pool, perform the following:

1. **Log on to the BBI as administrator user.**
2. **From the System tree view, select VPN Gateways.**

   The VPN Gateways form appears.
3. **Select the configured VPN for which you want to enable Host IP Pool.**

   The VPN Summary form appears.
4. **Select Host IP Pool.**

   The status form appears.



HIP Pool

Lets you enable or disable Host based IP Pool menu..

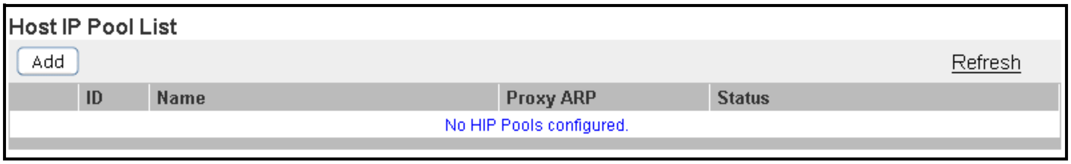
Status: enabled

5. **From the Status list, select enabled.**
6. **Click Update.**

   The VPN Summary form appears with the Host IP Address Pool option.

7. **Select the Host IP Address Pool.**

   The Host IP Pool List form appears.

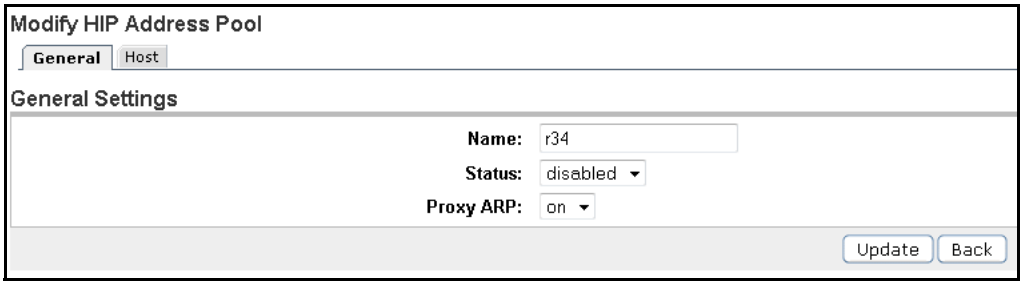


Host IP Pool List

	ID	Name	Proxy ARP	Status
No HIP Pools configured.				

8. **Click Add.**

   The Add new IP Address Pool form appears.



Modify HIP Address Pool

General Settings

Name: r34

Status: disabled

Proxy ARP: on

9. **From the HIP Pool ID list, select HIP Pool ID.**

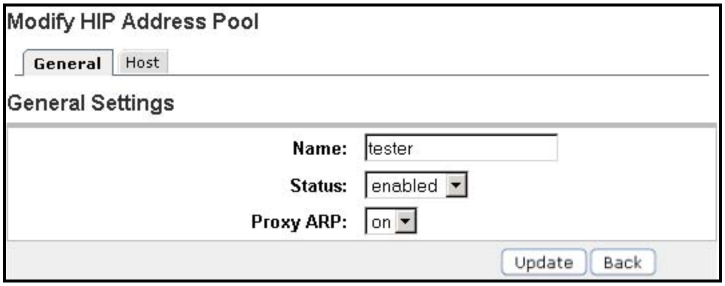
10. **In the Name field, enter the HIP Pool name.**

11. **From the Status list, select `enabled`.**

12. **From the Proxy ARP list, select `on`.**

13. **Click Update.**

    The Modify HIP Address Pool form appears.



Modify HIP Address Pool

General Settings

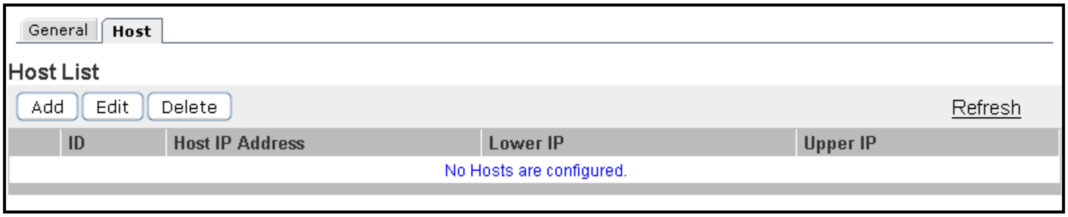
Name: tester

Status: enabled

Proxy ARP: on

14. **Click Host tab.**

    The Host List form appears.



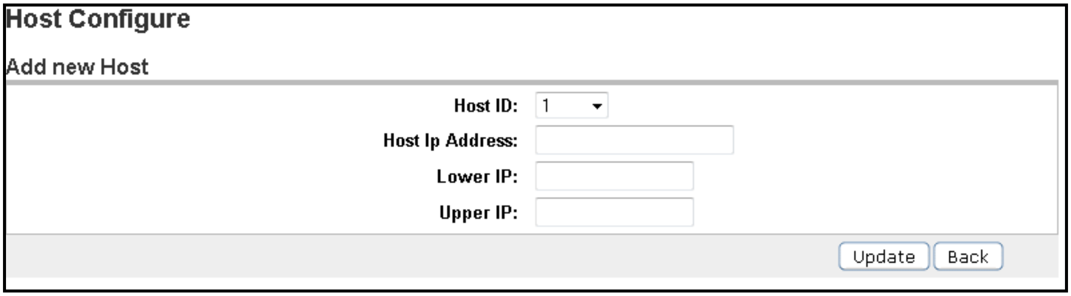
Host List

ID	Host IP Address	Lower IP	Upper IP

No Hosts are configured.

15. **Click Add.**

    The Add new Host form appears.



Host Configure

Add new Host

Host ID: 1

Host Ip Address:

Lower IP:

Upper IP:

16. **From the Host ID list, select Host ID.**
17. **In the Host Ip Address field, enter the Host IP address.**
18. **In the Lower IP field, enter the lower IP address of the range.**
19. **In the Upper IP field, enter the upper IP address of the range.**
20. **Click Update.**
21. **Apply changes.**

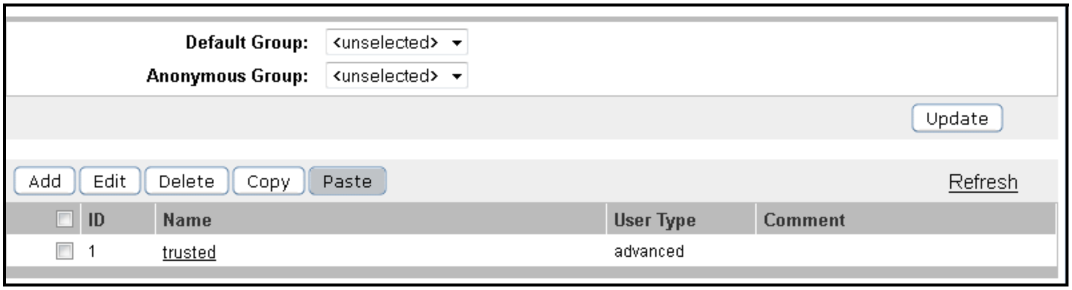
Map the IP Pool to User Group (Optional)

As mentioned on page 610, 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.

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. How to create a default IP Pool is described in the next section.

Follow these steps to map an IP Pool to a user group:

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on Groups settings.**
5. **Select the check box next to the group to which you want to map an IP Pool.**

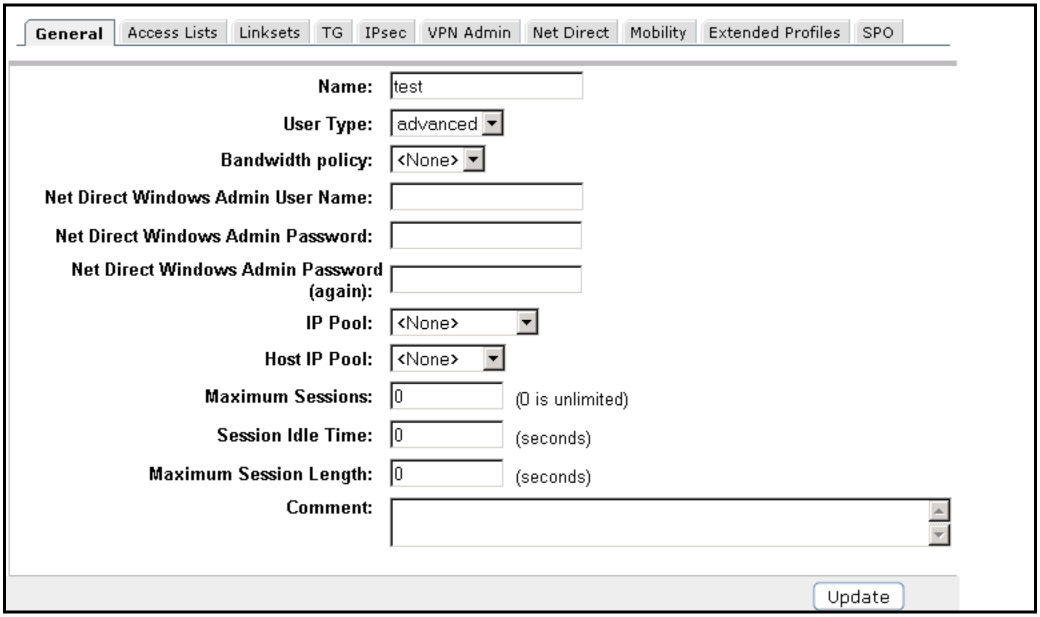


Default Group: <unselected>
Anonymous Group: <unselected>

□	ID	Name	User Type	Comment
□	1	trusted	advanced	

6. **Click Edit.**

7. **In the IP Pool list, select the IP Pool that you want to map to the current group.**



Name: test

User Type: advanced

Bandwidth policy: <None>

Net Direct Windows Admin User Name:

Net Direct Windows Admin Password:

Net Direct Windows Admin Password (again):

IP Pool: <None>

Host IP Pool: <None>

Maximum Sessions: 0 (0 is unlimited)

Session Idle Time: 0 (seconds)

Maximum Session Length: 0 (seconds)

Comment:

8. **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 Avaya VPN Client (SSL) clients.

Enable Avaya VPN Client (SSL)

1. **Log in to the BBI as administrator user.**

2. **Click on Config tab.**

3. **Click on the VPN gateway name.**

4. **Click on VPN Client settings.**

5. **Click Net Direct Client.**

6. **In the the Net Direct Client list box, select the desired option.**

   - `on`: Avaya VPN Client (SSL) client access is enabled for all users in the current VPN, that is, the client can be downloaded from the Portal provided a Avaya VPN Client (SSL) link has been created on the Portal's Home tab.
   - `off`: Avaya VPN Client (SSL) client access is disabled.
   - `group`: Lets you delegate to group level whether or not Avaya VPN Client (SSL) client access should be allowed. To enable Avaya VPN Client (SSL) client access for members of a specific group, go to the **VPN Gateways>VPN #>Group Settings>Groups>General** form, display the desired group and select `on` in the Avaya VPN Client (SSL) client list box.

   When Avaya VPN Client (SSL) is enabled (that is, set to `on` or `group`), the other fields and list boxes in the form become editable. Avaya VPN Client (SSL) will work fine with the default settings so you do not normally have to change the settings (listed in Step 7 to Step 13):

7. **In the Idle Check list box, select the desired option.**

   - `on`: The Avaya VPN Client (SSL) connection is terminated if the session is idle, when the user exits Avaya VPN Client (SSL), logs out from the Portal, reloads the Portal or closes the browser window. This is the default value.
   - `off`: The Avaya VPN Client (SSL) connection is only terminated when the user exits Avaya VPN Client (SSL), logs out from the Portal, reloads the Portal or closes the browser window.

8. **In the Retry Connection Time field, enter the desired value.**

   This setup sets the maximum timeout for reconnection if the Avaya VPN Client (SSL) connectivity to the server is lost. Reconnection helps restore the Avaya VPN Client (SSL) session without user intervention.

   The default value is 180 seconds (3 minutes). If you set it to 0, the service will be disabled. The valid range is 60-3600 seconds, that is, 1minute to 60 minutes.

The field is editable only if Avaya VPN Client (SSL) Client is on.

9. **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 Avaya VPN Client (SSL) client and the Avaya 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 Avaya VPN Client (SSL) clients are allowed.

10. **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 Avaya VPN Client (SSL) client and the Avaya 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 Avaya VPN Client (SSL) clients are allowed.

11. **In the UDP Ports field, enter the desired UDP port range.**

    This step lets you configure UDP ports to be used by the Avaya VPN Client (SSL) client. The Avaya VPN Client (SSL) client uses configured ports for sending encrypted UDP packets to the Avaya VPN Gateway. If this fails (due to for example firewalls between the client and the Avaya 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.

    To disable the UDP ports, the port range 0-1 needs to be specified.

12. **In the MSS Clamping list box, verify that the desired setting is selected.**

    - `on`: The Avaya VPN Gateway 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 Avaya VPN Gateway 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 are subject to fragmentation. This results in a slower connection.

13. **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 Avaya VPN Client (SSL) client is not allowed to connect to the Avaya VPN Gateway. The default value is `all`, that is, no restrictions apply.

- `all`: All Avaya VPN Client (SSL) client connections are allowed, irrespective of what OS the client runs on.
- `generic_win`: Avaya VPN Client (SSL) clients running on any other Windows version are allowed to
connect.
- `linux`: Avaya VPN Client (SSL) clients running on Linux are allowed to connect.
- `mac`: Avaya VPN Client (SSL) clients running on Mac OS X are allowed to connect.
- `unknown`: Avaya VPN Client (SSL) clients running on an OS that cannot be identified (for example new OS
versions) are allowed to connect.
- `win2k`: Avaya VPN Client (SSL) clients running on Windows 2000 are allowed to connect.
- `winxp`: Avaya VPN Client (SSL) clients running on Windows XP are allowed to connect.

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

Banner Text

To configure a banner message to be displayed to the user when Avaya VPN Client (SSL) is successfully downloaded and/or installed, proceed as follows:

1. **Scroll down to the the Net Direct Banner text box.**

   Or click the Net Direct Banner in the gray area in the Net Direct Client Access Settings form.

2. **In the text box, enter or paste the desired banner text.**
3. **Click Update and apply the changes.**

   If no banner text is configured, the window will not be displayed.

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 Avaya VPN Gateway or directly to the Internet.

1. **Log in to the BBI as administrator user.**
2. **Click on Config tab.**
3. **Click on the VPN gateway name.**
4. **Click on VPN Client settings.**

5. **Select Split Networks.**

   .In the Split Tunnel Mode list box, select the desired split tunnel mode.

   - `disabled`. Tunnels all network traffic through the Avaya VPN Client (SSL) client to the Avaya VPN Gateway.
   - `enabled`. Tunnels traffic to *specified networks* (see the next step) to the Avaya 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 Avaya VPN Client (SSL) client to the Avaya 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 Avaya VPN Gateway. All other network traffic is tunneled through the Avaya VPN Client (SSL) client to the Avaya VPN Gateway. This is the default setting.

6. **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).

7. **Under Split Tunnel Network List, click Add. In the Network IP field, enter the network IP address to be tunneled.**

8. **In the Network Mask field, enter the desired network mask.**

9. **Click Update.**

10. **Add another network in the same way, by repeating Step 8 to Step 11.**

11. **Apply the changes.**

CHAPTER 22
Configure Portal Guard

The Portal Guard feature is an easy way of *converting* an existing HTTP site to generate HTTPS links, secure cookies and so on. The Avaya VPN Gateway not only handles the SSL processing but also ensures that all existing web links are rewritten to HTTPS. This eliminates the need to rewrite each link manually.

This feature can for example be used to accelerate an existing web Portal or any HTTP site where SSL offload and HTTP to HTTPS rewrite is the desired option. This site and any web sites or web applications launched from the site will now be available from the Internet through the Avaya VPN Gateway. All client traffic will be protected with SSL and internal applications and sites do not need to modified to support access from Internet clients. Access rules are used to limit which internal sites can be reached through Portal Guard.

When the Portal Guard feature is used, the Avaya VPN Gateway's authentication system is turned off. To access the backend web server, the remote user should enter the VPN Portal's IP address or host name. The user will then be redirected to the backend web server for authentication, without first having to log in to the VPN Portal.

NOTE – The Portal Guard feature is only available if a Portal Guard license has been loaded.

HTTP to HTTPS Rewrite

Using Portal Guard, any link that the remote user clicks while being logged in to the backend server is rewritten to include the Avaya VPN Gateway rewrite prefix.

Both relative site links (e.g. `/site/file.html`) and absolute site links (e.g. `http://inside.example.com/site/file.html`) will be rewritten.

The Avaya VPN Gateway rewrite prefix (boldface) is added to the link properties as shown:
https://vip.example.com/http/inside.example.com/site/file.html

Initial Setup

Before enabling Portal Guard feature you should perform an initial setup of the system. Set up the system as a one-armed configuration and run the VPN Quick Setup wizard. The initial setup procedure is described in Chapter 3, "Initial Setup" in the *User's Guide*.

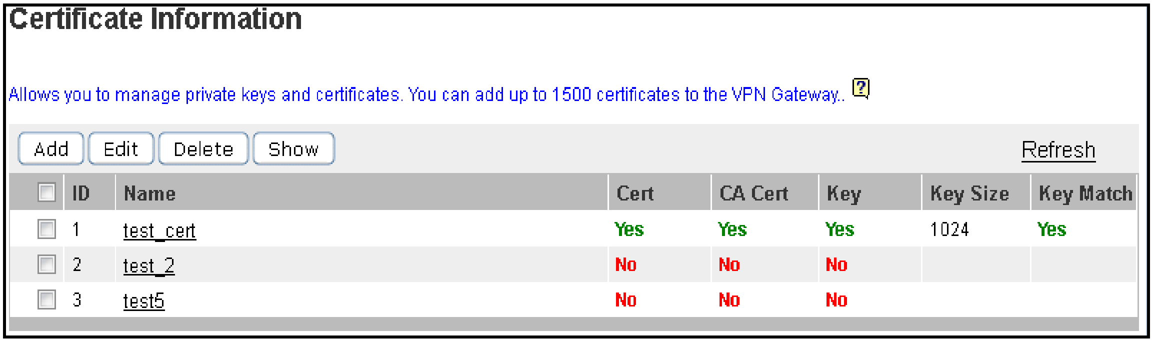
Running the VPN Quick Setup wizard will provide you with a basic configuration including a test user and a test certificate so that you can test that the VPN Portal is accessible. To view the other settings provided by the wizard, see Chapter 5, "Clientless Mode".

Import Signed Certificate to the Avaya VPN Gateway

This instruction assumes that you have a real server certificate available, signed by a CA authority. The certificate can be imported to the Avaya VPN Gateway as a file, through the BBI, or be pasted into the BBI as text.

1. **Logon to the BBI as administrator.**
2. **In the System tree view, select Certificates.**

   The test certificate created when you ran the VPN Quick setup wizard is displayed.



Certificate Information

Allows you to manage private keys and certificates. You can add up to 1500 certificates to the VPN Gateway..

□	ID	Name	Cert	CA Cert	Key	Key Size	Key Match
□	1	test_cert	Yes	Yes	Yes	1024	Yes
□	2	test_2	No	No	No		
□	3	test5	No	No	No		

3. **Click Add.**

   The new certificate will be assigned certificate number 2.

4. **Enter an appropriate name for the certificate, for example server_cert.**
5. **Click Update**

   A place holder for the new certificate is created.

6. **Click on the certificate created.**

Certificate summary screen is displayed.

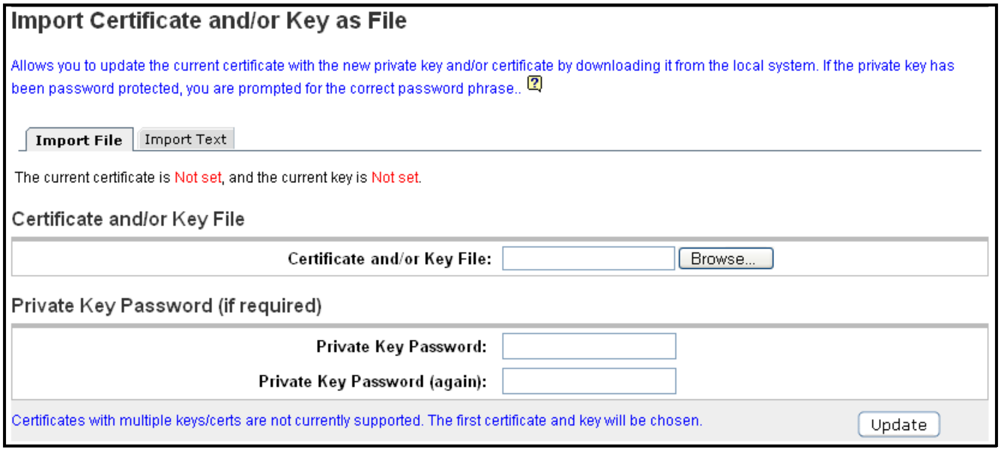
7. **Under Settings, select Import.**

   The Import Certificate and/or Key as File screen is displayed.

8. **To import a certificate file, select File.**

   You can also paste the certificate you wish to import. In this case, select Text instead of File.

   The Import Certificate as File form is displayed.



Import Certificate and/or Key as File

Allows you to update the current certificate with the new private key and/or certificate by downloading it from the local system. If the private key has been password protected, you are prompted for the correct password phrase..

The current certificate is Not set, and the current key is Not set.

Certificate and/or Key File

Certificate and/or Key File:

Private Key Password (if required)

Private Key Password:

Private Key Password (again):

Certificates with multiple keys/certs are not currently supported. The first certificate and key will be chosen.

9. **Under Certificate and/or Key file, click Browse.**

   The files in your file system are displayed.

10. **Double-click the certificate file you wish to import.**

11. **In the fields under Private Key Password, enter the import passphrase if required.**

12. **Click Update.**

13. **In the tree view, select Certificates to view the properties of the imported certificate.**

    The Certificate Information screen is displayed.

14. **Apply the changes.**

Map Signed Server Certificate to VPN

When the signed server certificate has been added to the Avaya VPN Gateway, it should be mapped to the portal server of the desired VPN. The certificate (with certificate no 1) that is currently mapped to your portal server is a test certificate. Select the number corresponding to the signed certificate that you have added to the Avaya VPN Gateway.

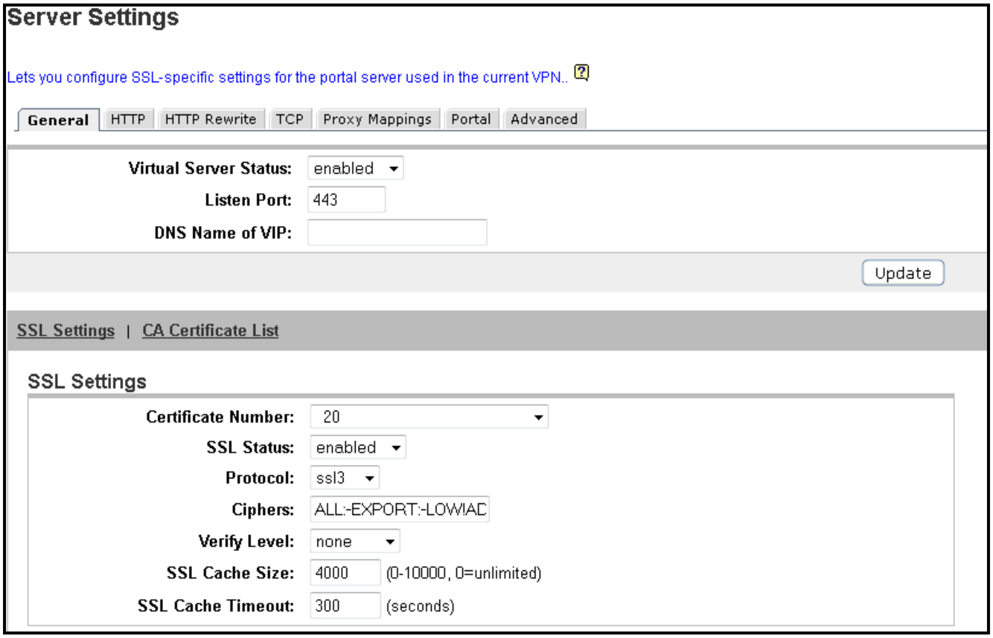
1. **In the System tree view, select VPN Gateways.**

   The VPN Summary screen is displayed.

2. **Under Settings, select SSL.**

   The Server Settings screen is displayed.

3. **Under General Settings, in the Certificate Number list box, select the certificate number you wish to map to the portal server.**



Server Settings

Lets you configure SSL-specific settings for the portal server used in the current VPN..

Virtual Server Status: enabled
Listen Port: 443
DNS Name of VIP:

SSL Settings

Certificate Number: 20
SSL Status: enabled
Protocol: ssl3
Ciphers: ALL:-EXPORT:-LOW:!AC
Verify Level: none
SSL Cache Size: 4000 (0-10000, 0=unlimited)
SSL Cache Timeout: 300 (seconds)

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

Update DNS Server

The local DNS server should be updated with the domain name used for the VPN, and be configured to perform reverse DNS lookups.

License Key

To enable the Portal Guard feature in the Avaya VPN Gateway software, a license key must be obtained from Avaya. To obtain the license keys, you have to provide the MAC address of each Avaya VPN Gateway for which a license should be installed.

For instructions on how to obtain the MAC address and how to paste the license key, see "Licenses" on page 73 in Chapter 4, "VPN Introduction".

Configure a Default Group

Remote users requesting the Avaya VPN Gateway Portal to reach the corporate web Portal will automatically be placed in a default group. Before you enable the Portal Guard feature you should configure this group on the Avaya VPN Gateway and provide the relevant access rules for the group.

NOTE – Be careful when defining the access rules for the default group so that user access is truly limited to the specified intranet web site and allowed links on that web site.

Instructions on how to configure groups and access rules in Chapter 8, "Groups, Access Rules and Profiles".

Configure Portal Acceleration

To configure portal acceleration of an existing Portal, proceed as follows:

1. **In the System tree view, select VPN Gateways.**

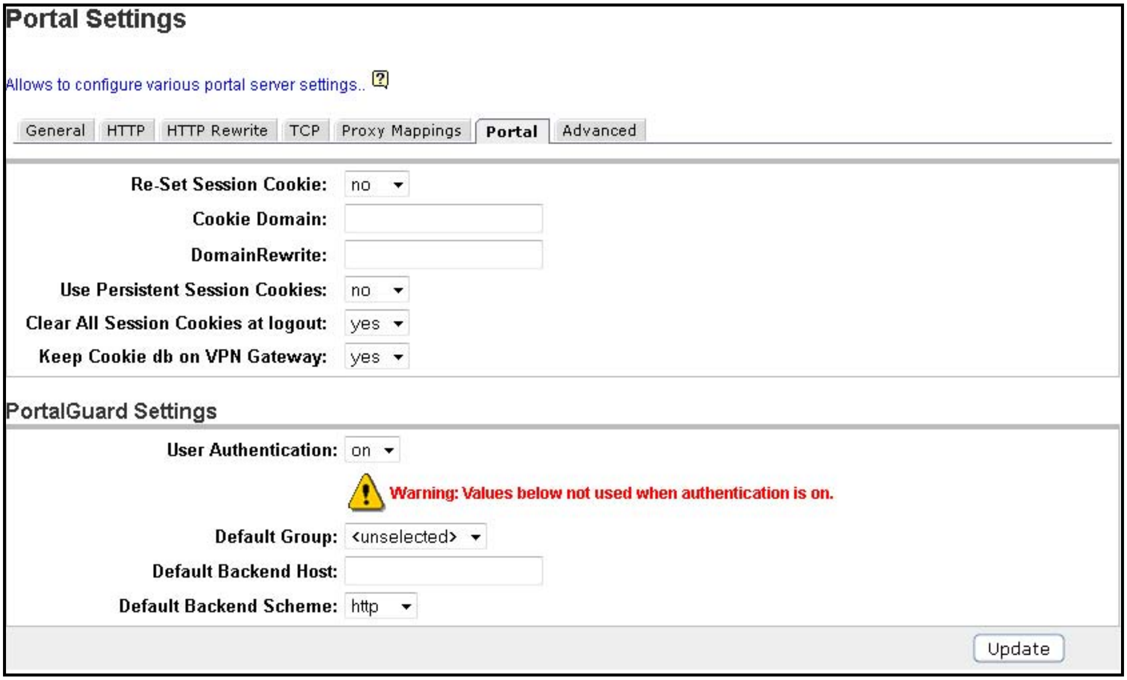
   The VPN Summary screen is displayed.

2. **Under Settings, select SSL.**

   The Server Settings screen is displayed.

3. **Click on the Portal tab.**

The Portal Settings form is displayed.



Portal Settings

Allows to configure various portal server settings..

Re-Set Session Cookie: no

Cookie Domain:

DomainRewrite:

Use Persistent Session Cookies: no

Clear All Session Cookies at logout: yes

Keep Cookie db on VPN Gateway: yes

PortalGuard Settings

User Authentication: on

Warning: Values below not used when authentication is on.

Default Group: <unselected>

Default Backend Host:

Default Backend Scheme: http

4. **Under Re-Set Session Cookie select the status from the drop-down list.**

5. **Click Update.**

6. **Apply the changes.**

CHAPTER 23
SSL VPN Cluster Manager

The SSL VPN Cluster Manager is a Java-based application that works as a minimum administering tool that is the user will be able to configure some of the options available in the BBI or CLI by providing status update as well as configuration of VPN Gateway clusters.

The main features of the SSL VPN Cluster Manager are:

- Location-based hierarchical tree view of clusters. Create your own hierarchy in the SSL VPN Manager tree view by adding geographical domains where existing clusters and hosts can be included.
- Multi-level node views. Expand the SSL VPN Network node (top node) to view existing domains. Expand a domain to view included clusters. Expand a cluster to view connected hosts.
- Software/configuration management. Upgrade several clusters with a new Avaya VPN Gateway software version at the same time. Export and import configurations across clusters.
- VPN synchronization. Copy configurations from one VPN to another within a cluster or across different clusters.
- Performance graphing. View memory and CPU usage and different license usage (SSL, IPSEC, SPIKE, SPO, ALL LICENSE USAGE) per cluster or host. View current sessions per cluster. The information is displayed as graphs that can be customized and saved.
- Centralized user administration. Manage administrator user accounts for several clusters at the same time.
- Alarms view displaying alarms generated for all clusters or for specific clusters.

The SSL VPN Cluster Manager stores the configuration and authentication information in the local client system where the BBI is launched.

The user has to authenticate to the SSL VPN Cluster Manager before using it.

Start the SSL VPN Cluster Manager

1. **Logon to the BBI as administrator.**

2. **Click on Config tab.**

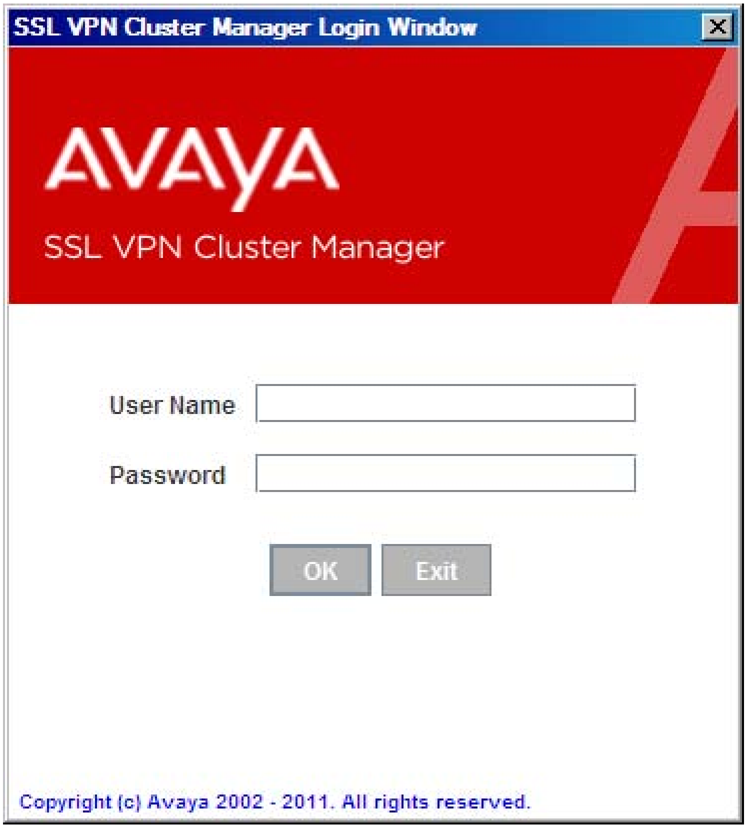
3. **Select Cluster Manager.**

   The SSL VPN Cluster Manager form is displayed.

4. **Click Launch.**

5. **Install the Java applet when prompted.**

   The SSL VPN Cluster Manager Login window is displayed.



SSL VPN Cluster Manager Login Window
AVAYA
SSL VPN Cluster Manager
User Name
Password
OK
Exit
Copyright (c) Avaya 2002 - 2011. All rights reserved.

6. **Log in with the administrator user name and password.**

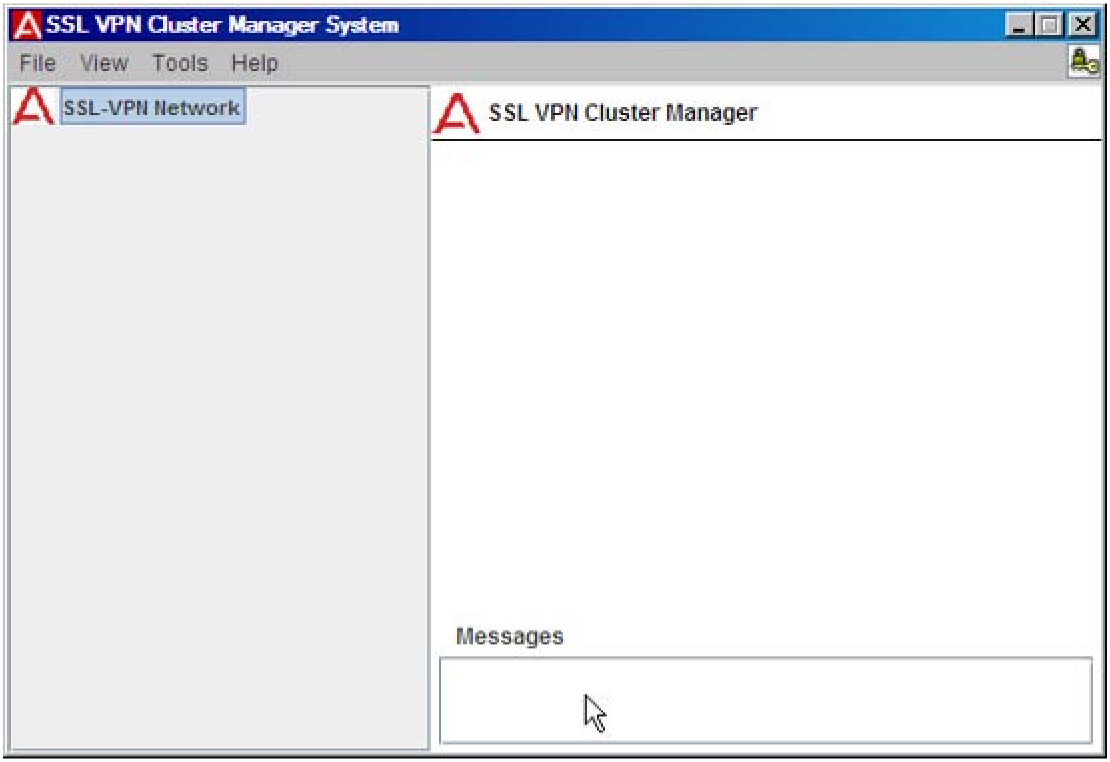
   The default user name and password is `admin`/`admin`.

The SSL VPN Cluster Manager maintains its own user authentication information, that is, the user name and password information is not synchronized with the BBI. Once logged in to the SSL VPN Cluster Manager, you can change the password (see "Change SSL VPN Cluster Manager Password" on page 671).

The SSL VPN Cluster Manager does not support RADIUS challenge-based authentication, only regular authentication is supported.

7. **Install the Java applet when prompted.**

   The SSL VPN Cluster Manager System window is displayed.



The first time you start the SSL VPN Cluster Manager, no cluster information is displayed. You will have to add domains and cluster to the SSL VPN Network tree view yourself.

Set Idle Timeout

Set the desired idle timeout for the SSL VPN Cluster Manager.

1. **On the View menu, select Cluster Manager Timeout.**

2. **Enter the desired timeout value in minutes and click OK.**

Configure the Cluster Manager

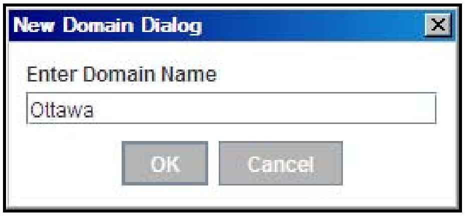
Add Domain or Region

To achieve logical grouping of your devices (for example based on location), you can add a domain or region to the SSL VPN Network tree.

1. **In the SSL VPN Network tree, select the SSL VPN Network top level root node.**

   If you have previously created domains or regions, you may select an existing domain/region under which you want to create a new domain/region.

2. **On the File menu, select Add Domain.**

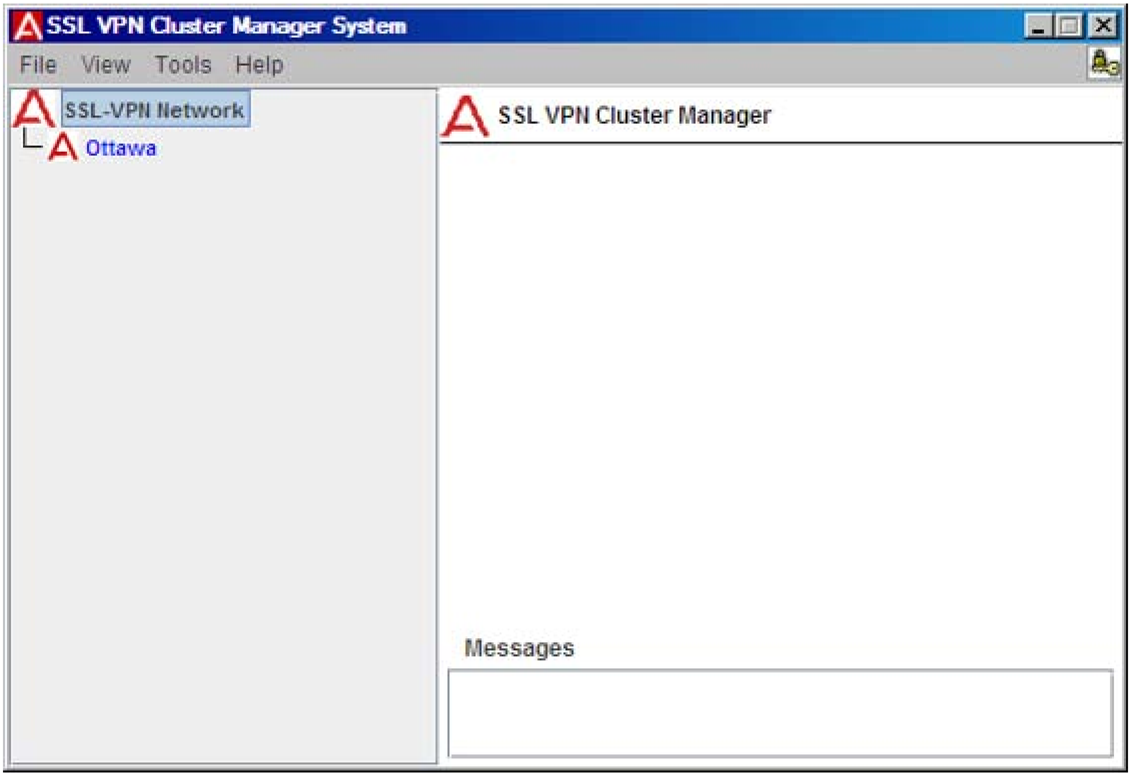


Ottawa

3. **Enter the domain name.**

4. **Click OK.**

The domain name is added to the SSL VPN Network tree under the selected node.



You can add either domains or clusters under this newly created domain to achieve logical grouping.

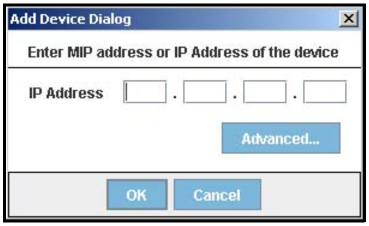
Add Cluster

This function lets you add a symbol representing a cluster of Avaya VPN Gateways. The SSL VPN Manager automatically discovers the hosts (Avaya VPN Gateways) contained in the cluster and creates the

corresponding nodes under the cluster symbol in the SSL VPN Network tree view.

1. **In the SSL VPN Network tree view, select the domain (or the SSL VPN Network root node) where you want to place the new cluster.**

2. **On the File menu, select Add Device.**



3. **Enter the MIP (Management IP) address of the cluster you want to add.**

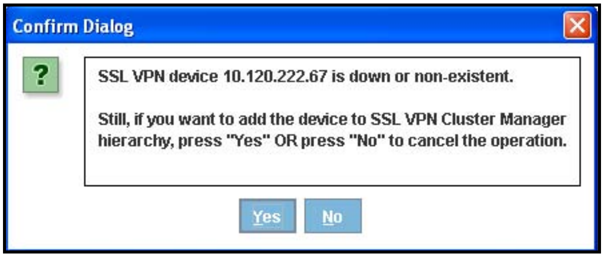
   As an alternative, enter the IP address of any of the Avaya VPN Gateway hosts contained in that cluster.

   Click **Advanced** to open a window where you can change certain default parameters (Protocol, Port and so on) used by the SSL VPN Cluster Manager to communicate with the cluster. For example, if you are using HTTP to communicate with the cluster, change the **Protocol** value from HTTPS to HTTP.

4. **Click OK.**

   If the specified cluster is up, the SSL VPN Cluster Manager will detect the devices contained in the cluster and create the corresponding nodes under the cluster symbol.

   If the cluster is down, the SSL VPN Cluster Manager displays the following message:



SSL VPN device 10.120.222.67 is down or non-existent.

Still, if you want to add the device to SSL VPN Cluster Manager hierarchy, press "Yes" OR press "No" to cancel the operation.

   If you still want to add the cluster node to the SSL VPN Network tree view, click **Yes**. Otherwise click **No**.

5. **Add another cluster (if any) by repeating Step 2 to Step 4.**

Tree View with Clusters Added

When a cluster of Avaya VPN Gateways has been added to the SSL VPN Network tree view, the color of the domain, cluster and host texts indicate the status of hosts contained in the domains or clusters. The Cluster Manager periodically polls the clusters and updates the host status. The status of the host is then propagated to the root node in the SSL VPN Network tree view.

Color/Icon	State
Green	Domain/Cluster: All hosts in the domain/cluster are in up state. Host: Host is in up state.
Orange	Domain/Cluster: One or more hosts in the domain/cluster have reached warning level for CPU or memory utilization (75%). Host: Host has reached warning level for CPU or memory utilization.
Orange (with blinking icon)	Domain/Cluster: One or more hosts in the domain/cluster are in down state, or have reached critical level for CPU or memory utilization (90%). Host: Host has reached critical level for CPU or memory utilization.
Red (with blinking icon)	Domain/Cluster: All hosts in the domain/cluster are in down state. Host: Host is in down state.
Blue	Information has not yet been loaded. Domain has no clusters.
⊗	Displayed next to cluster node if an authentication error occurs when SSL VPN Cluster Manager is polling the cluster.

The blinking effect is propagated in such a way that the lowest visible node (Domain/Cluster/Host) is shown with corresponding blinking icon.

Cluster Management

Having added the desired clusters to the SSL VPN Network tree view, you can view/manage information for

- multiple clusters
- a single cluster

Different tabs are displayed on the SSL VPN Cluster Manager’s right pane depending on if one or more clusters are selected in the SSL VPN Network tree view.

Multiple Clusters

To display cluster information for multiple clusters, select the desired cluster nodes (using CTRL-click) in the SSL VPN Network tree view on the left pane.

On the right pane, selected clusters are listed in the table. The current Avaya VPN Gateway software version for the different clusters is displayed in the **Image** column.

Install Software Image

Using this function, you can upgrade several clusters to a new software version.

1. **Click File.**

   The SSL VPN Update Package window opens.

2. **Find the software image that you wish to install and click Open.**

3. **Back in the SSL VPN Cluster Manager System window, in the Image Update area, click Install.**

   During installation, the following status window is displayed:

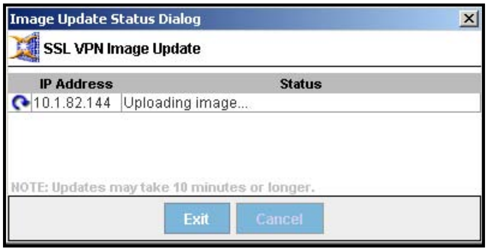


Image Update Status Dialog

SSL VPN Image Update

IP Address	Status
10.1.82.144	Uploading image...

NOTE: Updates may take 10 minutes or longer.

4. **When the status is “Image Activated”, click Exit.**

   The software version is updated.

To install a new software image for a specific cluster, see “Install Software Image” on page 656. New software images can also be installed through **Operation>Image Update** in the BBI.

Export Configuration

Using this function, you can export the current configuration of several clusters to separate files. Private keys and certificates are included.

1. **Select the Config Export/Import tab.**

   Selected clusters are listed on the right pane. Note that only the clusters for which the user has administrator access are displayed. If the user does not have administrator access to any of the selected clusters, the Selected Clusters table is empty.

2. **Click ▼ on the desired cluster row to display the Configuration window, where you can specify a folder and a file name for the cluster's configuration file.**

3. **Click ▼ on the next cluster row to specify folder/file name for that cluster's configuration file as well.**

4. **In the Secret Key field, enter the secret key used to encrypt the configuration files.**

   Note that the secret key is case-sensitive. The key must be supplied when the configuration files are imported to the clusters.

5. **Click Export.**

Import Configuration

1. **Click ▼ on the desired cluster row to display the Configuration window, where you can select a folder and a configuration file to import to the current cluster.**
2. **Click ▼ on the next cluster row to select a configuration file to import to this cluster.**
3. **In the Secret Key field, enter the secret key used to decrypt the configuration files.**

   Note that the secret key is case-sensitive. The same key that was used to export the files should be used to import the files to the cluster(s).

4. **Click Import.**

Copy Configuration to Other VPN Across Clusters

Using this function, you can copy configuration from one VPN to another, within the same cluster or across different clusters.

1. **Select the Bulk Config tab.**
2. **In the VPN Synchronization area, in the Primary Cluster list box, select the cluster whose VPN you wish to copy the configuration from.**
3. **Click Wizard.**

   The Bulk Configuration of SSL VPN window is displayed.

   By default, the left pane shows an overview of VPN 1’s configuration for the selected cluster. To display configuration information for another VPN, select the desired VPN in the VPN list box. The VPN you select on the left pane will be the source VPN, that is, the VPN from which you wish to copy configuration information.

4. **To display a more detailed view of the configuration, click Details.**

NOTE – The SSL VPN Cluster Manager does not export all the parameters of the selected VPN to destination VPNs. Synchronization is only supported for *Linksets, Portal, Network, Authentication* and *Groups* set of parameters. Also note that the actual IP addresses of the VPN, the IPsec configuration, the Certificates, the local users information, and so on. which are all specific to individual VPNs are not exported.

---

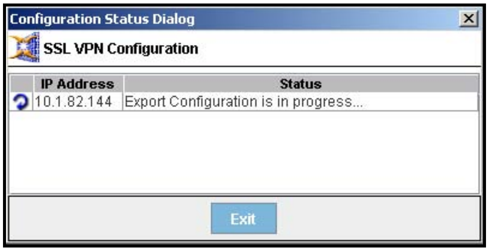
5. **Expand the desired connector to view the contents of each folder.**
6. **Click Close.**
7. **On the right pane, expand the desired clusters to view available target VPNs.**

8. **In the Selection column, check the check box next to the desired VPN(s).**

   These are the target VPNs, that is, the VPNs to which you wish to copy the configuration information.

9. **Click Export.**

   A status window is displayed.



Configuration Status Dialog

SSL VPN Configuration

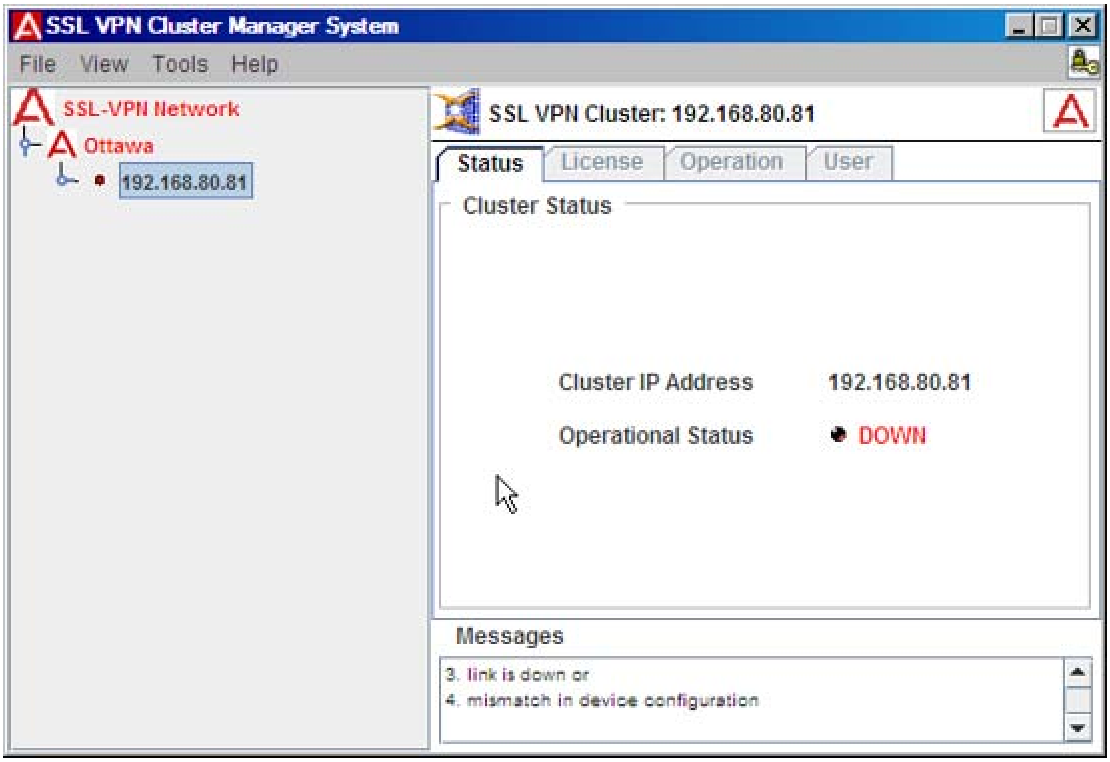
IP Address	Status
10.1.82.144	Export Configuration is in progress...

   When the SSL VPN Cluster Manager has finished copying, the status is changed to “Successfully Exported”.

10. **Click Exit.**

Single Cluster

To display information for a single cluster, select the desired cluster node in the SSL VPN Network tree view on the left pane.



Cluster IP Address 192.168.80.81

Operational Status ● DOWN

3. link is down or
4. mismatch in device configuration

To display hosts contained in a cluster, double-click the cluster symbol or expand the connector associated with the cluster node.

To refresh the right pane so that the latest information is displayed, click the Avaya VPN Client symbol.

Status Tab

The Status tab shows status information for the selected cluster, for example the status of individual hosts and which protocols and ports that can be used to access the cluster.

Host Status

IP Address	IP address of host in cluster.
MAC Address	MAC address of the host

Status

Up/down state.

MIP

Shows which host that currently holds the floating MIP (management IP address).

CPU %

Shows CPU usage.

Memory %

Shows memory usage.

Security Status

SSL

Shows whether or not access to the cluster is enabled through HTTP. HTTP access is enabled/disabled under **Administration>Web** in the BBI.

Web

Shows whether or not access to the cluster is enabled through HTTP. HTTP access is enabled/disabled under **Administration>Web** in the BBI.

SSH

Shows whether or not SSH access to the cluster is enabled. SSH access is enabled/disabled under **Administration>Telnet-SSH** in the BBI.

Telnet

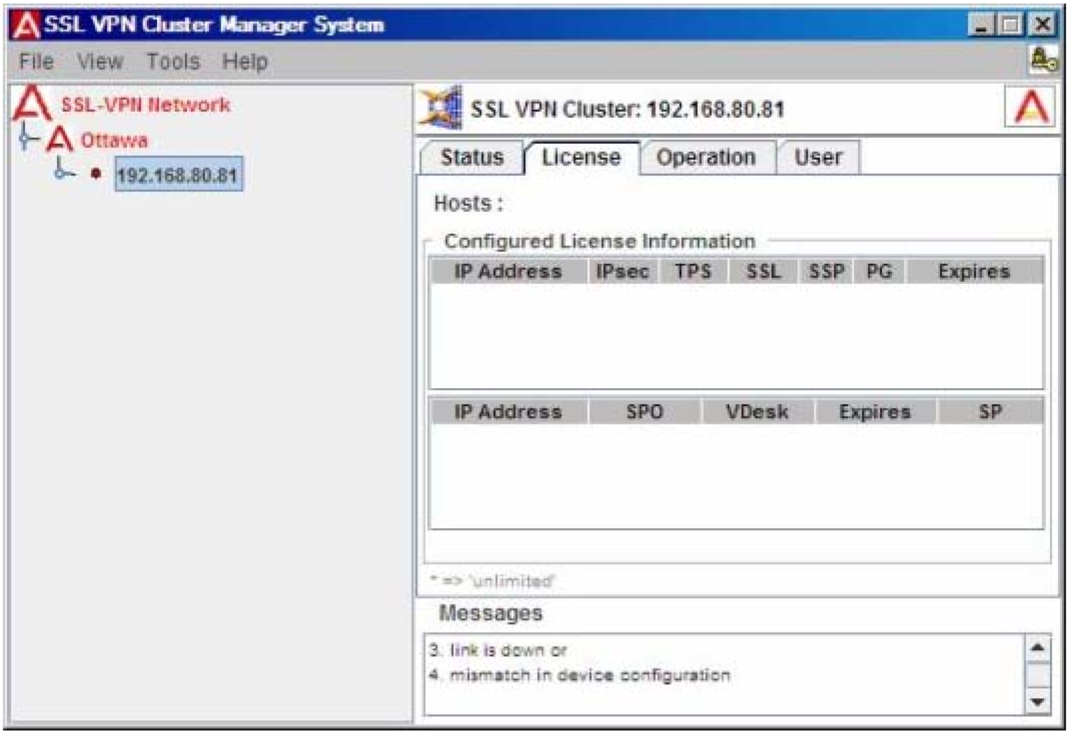
Shows whether or not Telnet access to the cluster is enabled. Telnet access is enabled/disabled under **Administration>Telnet-SSH** in the BBI.

Access List

Lists networks that are allowed to connect to the cluster. If the list is empty there are no restrictions. The access list can be edited under **Administration>Access List** in the BBI.

License Tab

All VPN Gateways that are up and running in a cluster contribute to the license pool. The License Tab shows these license information.



IP Address	IPsec	TPS	SSL	SSP	PG	Expires

IP Address	SPO	VDesk	Expires	SP

* => 'unlimited'

3. link is down or
4. mismatch in device configuration

IP Address - IP address of host in cluster.

IP Sec - Number of licenses for IPsec users

TPS - Number of Licenses for TPS users

SSL - Number of Licenses for SSL users

SSP - Shows on/off state

PG - Shows on/off state

Expires - Shows the expiry date of the license

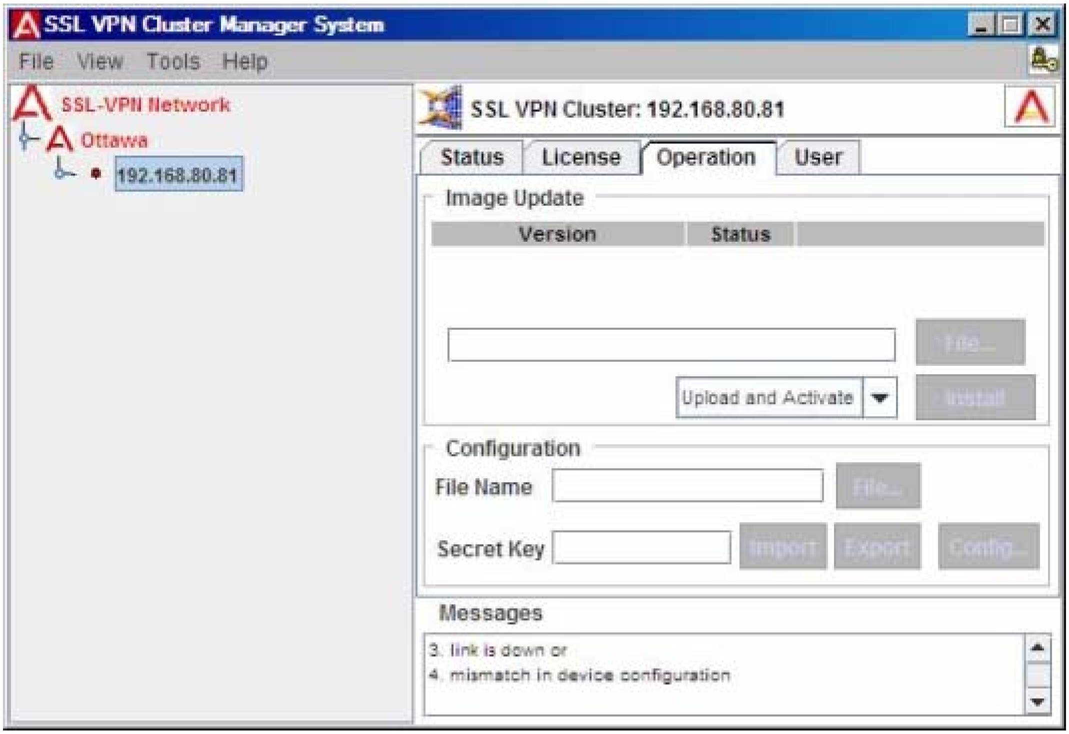
SP - Number of Licenses for SP users

SPO- Number of Licenses for SPO users

Vdesk- Number of Licenses for VDESK users

Operation Tab

The Operation tab lets you view which software version is running on the selected cluster, as well as install new software images. You can also export and import configuration files and copy configurations from one VPN to another, within the selected cluster.



3. link is down or
4. mismatch in device configuration

To manage software images and configuration export/import for *several clusters* at the same time, see the section “Multiple Clusters” on page 649. This also where you can find instructions on how to copy configurations from one VPN to another, across several clusters.

The **Operation** tab is only available to SSL VPN Manager users who are **Admin** users.

Install Software Image

1. **In the Image Update area, click File.**

   The SSL VPN Update Package window opens.

2. **Find the software image that you wish to install and click Open.**

3. **Back in the SSL VPN Cluster Manager System window, in the list box to the left of the Install button, select whether the software image should be uploaded *and* activated or just uploaded.**

   If you select **Upload and Activate**, the software image will be activated as soon as it is uploaded, that is, replace the previous software image.

   If you select **Upload Only**, you can activate the image later, using the Activate button.

4. **Click Install.**

   During installation, the following status window is displayed:

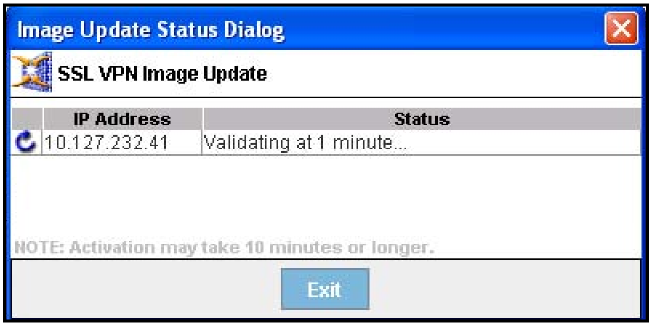


Image Update Status Dialog

SSL VPN Image Update

IP Address	Status
10.127.232.41	Validating at 1 minute...

NOTE: Activation may take 10 minutes or longer.

5. **When the status is “Image Activated/Uploaded”, click Exit.**

   The newly installed software image is displayed as a new row in the table in the Image Update area. The version number is displayed in the **Version** column.

   If you selected the option **Upload and Activate** before installing the image, the software image is automatically activated and the status is set to **permanent**. The status of the previously permanent version has changed to **old**.

   If you selected the option **Upload Only**, the status of the uploaded software image is **unpacked**. It can be activated by clicking the **Activate** button (see next section).

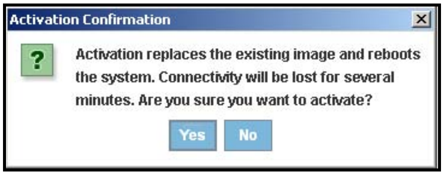
   New software images can also be installed through **Operation>Image Update** in the BBI.

Activate Software Image

Using this function you can activate unpacked or old software versions.

1. **To activate the software image, click Activate.**

   The following message is displayed.



Activation Confirmation

Activation replaces the existing image and reboots the system. Connectivity will be lost for several minutes. Are you sure you want to activate?

2. **To proceed with the activation, click Yes.**

   During activation, the following status window is displayed:

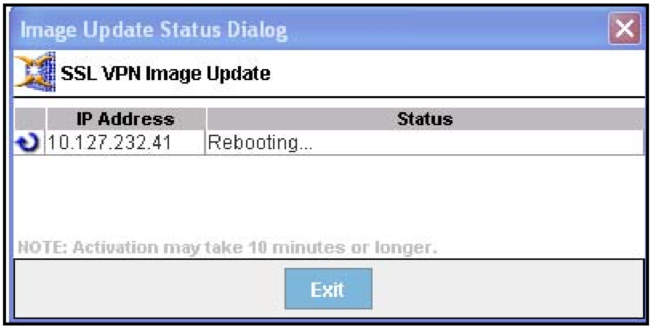


Image Update Status Dialog

SSL VPN Image Update

IP Address	Status
10.127.232.41	Rebooting...

NOTE: Activation may take 10 minutes or longer.

3. **When the status is “Image Activated”, click Exit.**

Export Configuration

Using this function, you can export the current cluster configuration, including private keys and certificates.

1. **In the Configuration area, click File.**

   The SSL VPN Configuration window is displayed.

2. **Save the file in the desired folder with the desired file name and click Open.**

3. **Back in the SSL VPN Cluster Manager System window, in the Secret Key field, enter a secret passphrase.**

   This will ensure that the configuration file cannot be imported or opened by unauthorized persons.

4. **Click Export.**

   The configuration can also be exported under **Operation>Configuration** in the BBI.

Import Configuration

Using this function, you can import a previously exported configuration file.

1. **In the Configuration area, click File.**

   The SSL VPN Configuration window is displayed.

2. **Find the file and click Open.**

3. **Back in the SSL VPN Cluster Manager System window, in the Secret Key field, enter the secret passphrase that was used when exporting the configuration file.**

4. **Click Import.**

   The configuration can also be imported under **Operation>Configuration** in the BBI.

Copy Configuration to Other VPN

Using this function, you can copy configuration from one VPN to another, within the cluster.

1. **On the Operation tab, click Config.**

   The Bulk Configuration of SSL VPN window is displayed.

   By default, the left pane shows an overview of VPN 1's configuration. To display configuration information for another VPN, select the desired VPN in the VPN list box. The VPN you select on the left pane will be the source VPN, that is, the VPN from which you wish to copy configuration information.

2. **To display a more detailed view of the configuration, click Details.**

NOTE – The SSL VPN Cluster Manager does not export all the parameters of the selected VPN to destination VPNs. Synchronization is only supported for *Linksets, Portal, Network, Authentication* and *Groups* set of parameters. Also note that the actual IP addresses of the VPN, the IPsec configuration, the Certificates, the local users information, and so on. which are all specific to individual VPNs are not exported.

3. **Expand the desired connector to view the contents of each folder.**

4. **Click Close.**

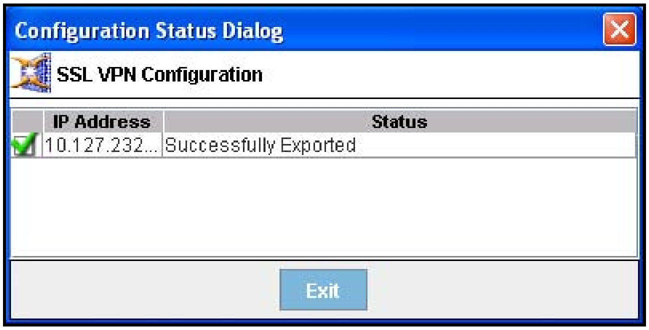
5. **On the right pane, expand the cluster connector to view available target VPNs.**

6. **In the Selection column, check the check box next to the desired VPN.**

   This is the target VPN, that is, the VPN to which you wish to copy the configuration information.

7. **Click Export.**

   A status window is displayed.



	IP Address	Status
✓	10.127.232...	Successfully Exported

   When the SSL VPN Cluster Manager has finished copying, the status is changed to “Successfully Exported”.

8. **Click Exit.**

Show Host Information

To display information about a single host, proceed as follows:

1. **In the SSL VPN Network tree view, expand the desired domain and cluster.**
2. **Select a host.**

   The Status tab is displayed on the right pane.

Status Information

IP Address	IP address of host.
Type	Master or Slave.
Memory %	Shows memory usage.
Status	Up/down state.
MIP Owner	True = the host currently holds the floating MIP (management IP address).
CPU %	Shows CPU usage.

Ports Information

Port Number	Port numbers on host.
Link Status	Up= When the Interface is configured for the corresponding Port.
>	Down = When the interface is not configured for the corresponding Port.
Autonegotiate	On = Ethernet autonegotiation enabled.
Speed	Port speed (Mbits/sec).
Mode	Duplex mode (full/half).

Interface(s) Information

Id	Host interface ID. A host can communicate on several network interfaces, each represented by an ID number.
IP Address	Host interface IP address.
VLAN Id	The host interface’s VLAN ID (if any). VLAN IDs can be used to increase the number of interfaces on a host if the there are not enough ports.

Mode
Failover or trunking. In failover mode, only one link is active at any given time. If a link is active on a port that fails, the active link is immediately switched over to one of the other configured ports. When failover mode is selected, a primary port may also have been specified.

Port(s)
Port(s) assigned to the interface.

Primary Port
If a failure of the active link occurs on the primary port, the active link is immediately transferred to a remaining (secondary) port. As soon as the primary port regains functionality, the active link will be transferred back to that port. The default primary port value is `0` (zero), indicating that the currently active link remains in use until the port fails, when the link is transferred to the other port. The link will remain active on the port to which it was transferred, even if the port that failed regains functionality. The primary port setting only has effect when more than one port is configured in the selected interface.

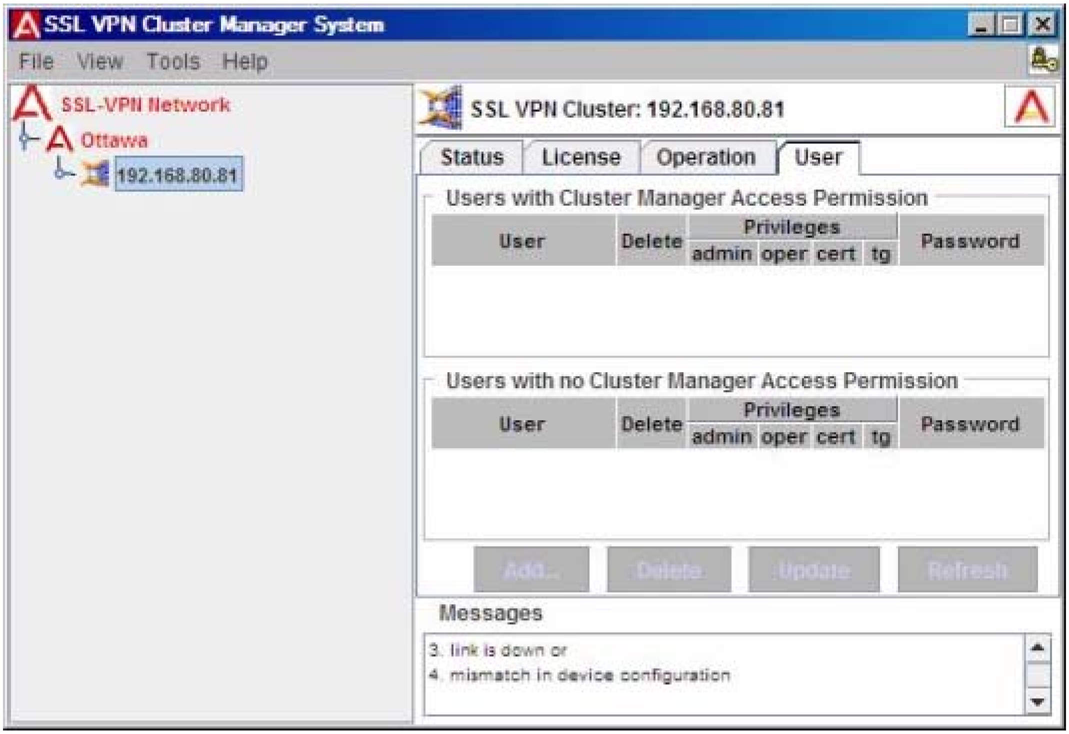
User Management

From the Cluster Manager's point of view, there are two types of administrator users:

- ***Users with no Cluster Manager Access Permission***. Administrator users that are *only* registered in the VPN Gateway software, that is, through the CLI under `/cfg/sys/user` or through the BBI under **Administration>Users**. These users cannot log in to the SSL VPN Cluster Manager unless they are explicitly given access (see "Convert User" on page 666).
- ***Users with Cluster Manager Access Permission***. Administrator users that are registered as users of the SSL VPN Cluster Managers *as well as* the VPN Gateway software. By default, the `admin` and `oper` users are also administrator users of the SSL VPN Cluster Manager.

The User Tab

The User tab lets you view administrator users for a cluster that is selected in the SSL VPN Network tree view.



3. link is down or
4. mismatch in device configuration

Under **Users with Cluster Manager Access Permission**, all users that have access to the selected cluster through the CLI/BBI *and* the SSL VPN Cluster Manager are listed. In the preceding example, the default `admin` and `oper` users are shown. These accounts are valid for SSL VPN Cluster Manager access by default.

You can view the details of the users in two ways:

- Navigate Tools > User Management
- Click on the User Management button at the top right corner of the SSL VPN Cluster Management window.

Under **Users with no Cluster Manager Access Permission**, any other administrator users registered in the cluster configuration are displayed. In the preceding example, `john` is allowed to log in to the cluster through the CLI/BBI, but he cannot log in to the SSL VPN Cluster Manager.

Change User Properties

SSL VPN Cluster Manager users that have been assigned **Admin** user privileges (access level specific to the SSL VPN Cluster Manager) can edit an administrator user's group membership and *cluster* password. The changes are saved in the Avaya VPN Gateway configuration.

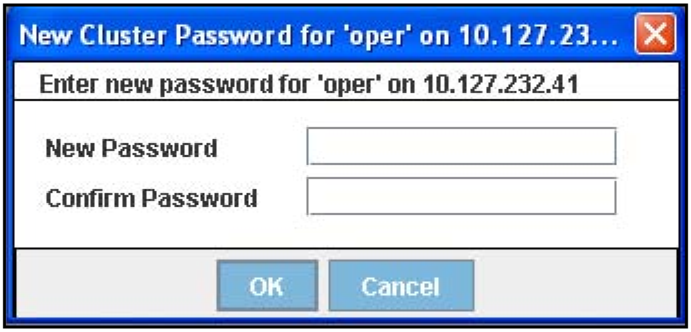
The default `admin` user is also by default **Admin** user in the SSL VPN Cluster Manager. The `oper` user is not **Admin** user in the SSL VPN Cluster Manager, which means that he/she cannot edit information about the **User** tab.

1. **To change the user's group membership, select the desired check box under `admin`, `oper`, `certadmin` and/or `tg` (Avaya Endpoint Access Control Agent).**

   This can be done under **Users with Cluster Manager Access Permission** (not for `admin` and `oper` users) as well as under **Users with no Cluster Manager Access Permission**. For information about the access rights for the various user groups, see the chapter "Managing Users and Groups" in the *User's Guide*.

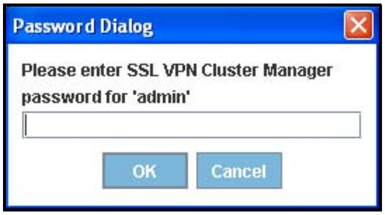
2. **To change a user's cluster password, click the empty box in the Password column next to the desired user.**

The cluster password is the password used to log in to the cluster through the CLI or BBI. You will be prompted for the cluster password if the cluster password cached for the logged in user in the SSL VPN Cluster Manager does not match the actual cluster password.


New Cluster Password for 'oper' on 10.127.23...
Enter new password for 'oper' on 10.127.232.41
New Password
Confirm Password
OK
Cancel

3. **Enter the new password in the fields and click OK.**

4. **Click Update.**



5. **Enter the Admin password and click OK.**

   The Admin password is the one that you used when you logged in to the SSL VPN Cluster Manager.

   The User Management Status window is displayed while the information is updated.

6. **When the status is changed to “Changed cluster password”, click Close.**

   Any information you have changed is also changed in the cluster configuration. For example, if you have changed the password, the user need to use this new password to log in to the CLI/BBI.

   However, changing the password of a **User with Cluster Manager Access Permission** (top table on the **User** tab), does not change the SSL VPN Cluster Manager login password for the selected user.

NOTE – When logging in to the SSL VPN Cluster Manager with a newly created user, after a password change and so on., the information might not yet have been completely propagated. This may result in error messages like “You don’t have access to the selected cluster(s)”.

Please allow the SSL VPN Cluster Manager some time to load before proceeding. If you get a message that the cluster is down, please check the protocol and port settings by selecting **Cluster Properties** on the **View** menu.

Delete User

1. **In the Delete column, select the check box on the row corresponding to the user that you wish to delete.**

   If the user cannot be deleted (as is the case with the `admin` and `oper` users), the check box is not displayed.

2. **Click the Delete button.**

   You are prompted for the Cluster Manager administrator password.

3. **Enter the password and click OK.**

4. **Confirm that you want to delete the user in the next window that is displayed.**

Convert User

A **User with no Cluster Manager Access Permission** (bottom table on the **User** tab) can be “converted” to a **User with Cluster Manager Access Permission** by means of drag and drop.

1. **In the bottom table, select the desired user and drag the object to the top table.**

   When the user later logs in to the SSL VPN Cluster Manager, he/she will have to authenticate to the cluster to be able to bring up the SSL VPN Network tree view. When prompted for a password, the *cluster* password should be used, that is, the user’s original password.

Add User to Single Cluster

This section describes another method of adding an SSL VPN Cluster Manager user. This method also lets you configure the user as an **Admin** user, that is, with privileges to install software images on the **Operation** tab and to manage users. The user is also added as administrator user in the CLI/BBI.

This instruction describes how to add a user to a single cluster. For instructions on how to add a user to several clusters at the same time, see “Add User to Multiple Clusters” on page 668.

1. **On the User tab, click Add.**

   The **Add User** window is displayed.

2. **In the User Id field, enter the new user’s user name.**

3. **In the password fields, enter the user's password.**

   This password will be valid *both* as a password for logging in to the SSL VPN Cluster Manager and as the cluster password. The user will be saved in the CLI/BBI with the supplied user name and password.

4. **In the Cluster Manager password of logged-in Administrator field, enter the administrator password.**

   This is the password you used when you logged in to the SSL VPN Cluster Manager as a user with **Admin** privileges.

5. **Check the Create As Administrator in Cluster Manager check box to make this user a user with Admin privileges in the SSL VPN Cluster Manager.**

   An **Admin** user has privileges to install software images on the **Operation** tab and to manage users.

   NOTE – You can also create a user without any privileges. These users can only login to the cluster manager but are not authorized to do cluster management configurations. You can view the details of these users, by clicking on the top right button (User Management) in the User Management window.

6. **Finally, check the groups to which the user should belong.**

   For information about the access rights for the various user groups, see the chapter "Managing Users and Groups" in the *User's Guide*.

7. **Click Add.**

   The User Management Status window is displayed while the information is updated.

8. **Click Close.**

   The user we have now added can log in to the SSL VPN Cluster Manager *and* to the CLI/BBI with the user name and password we entered in the **Add User** window.

Add User to Multiple Clusters

1. **On the Tools menu, select User Management.**

   The SSL VPN Cluster Manager User Management window is displayed.

2. **Click Add.**

   The **Add User** window is displayed.

3. **In the tree view on the left pane, expand the domain to view connected clusters.**

4. **Select the cluster you to which you want to add a user.**

   OR

   Select the domain to add the user to all clusters in the domain.

5. **Add the user according to the instructions in Step 2 to Step 8 in the previous section.**

Modify User

1. **On the Tools menu, select User Management.**

   The User Management window is displayed.

2. **Select the user whose properties you want to change.**

3. **Click Modify.**

   The Modify Users window is displayed.

4. **In the SSL VPN Network tree view, expand the desired domain and select the cluster for which the user information should be changed (or added).**

   If you select the root node (SSL VPN Network), changes will be added to all clusters in subordinated domains. If you select a domain, changes will be added to all clusters in the selected domain. If the user does not exist in a subordinated cluster, the user will be added to that cluster. If the user exists in a cluster, the user information will be changed.

5. **In the password fields, enter the user's password.**

   Specifying a password is only required if the user does not exist on all of the selected clusters. If you change the password here, only the *cluster* password is changed. The SSL VPN Cluster Manager password remains the same.

6. **Complete the remaining fields and check boxes as described in previous sections.**

7. **Click Modify.**

Delete User

This operation deletes the user from the SSL VPN Cluster Manager as well as from the CLI/BBI.

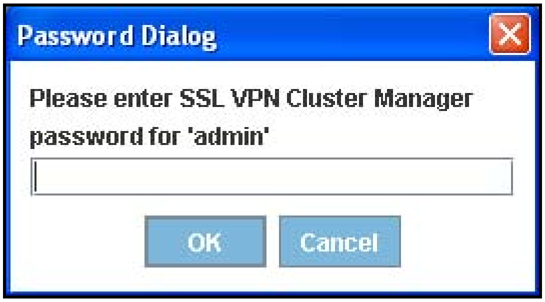
1. **On the Tools menu, select User Management.**

   The User Management window is displayed.

2. **Select the user you want to delete.**

3. **Click Delete.**

4. **The Password Dialog window is displayed.**



Password Dialog

Please enter SSL VPN Cluster Manager password for 'admin'

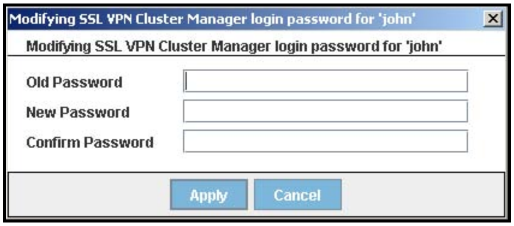
5. **Enter SSL VPN Cluster Manager password for admin.**

6. **Click OK.**

Change SSL VPN Cluster Manager Password

Using this function, the logged in user can change his/her password for accessing the SSL VPN Cluster Manager.

1. **On the Tools menu, select Change Login Password.**



Modifying SSL VPN Cluster Manager login password for 'john'

Modifying SSL VPN Cluster Manager login password for 'john'

Old Password

New Password

Confirm Password

2. **In the Old Password field, enter the current password.**

3. **In the New Password field, enter the new password.**

4. **In the Confirm password field, enter the new password once again.**

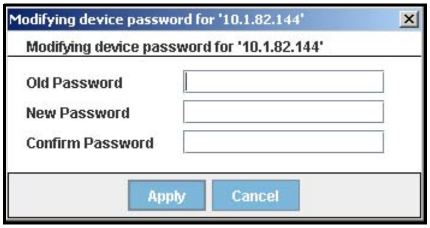
5. **Click Apply.**

Change Cluster Password

Using this function, the logged in user can change his/her password for accessing a specific cluster of Avaya VPN Gateways.

1. **In the SSL VPN network tree view, select the cluster for which the password should be changed.**

2. **On the Tools menu, select Change Device Password.**



Modifying device password for '10.1.82.144'

Modifying device password for '10.1.82.144'

Old Password

New Password

Confirm Password

3. **In the Old Password field, enter the current password.**

4. **In the New Password field, enter the new password.**

5. **In the Confirm password field, enter the new password once again.**

6. **Click Apply.**

Save Configuration to File

The SSL VPN Cluster Manager allows you to store the current SSL VPN Cluster Manager configuration by saving the contents to a file in XML format. This file can be loaded to the SSL VPN Cluster Manager at a later point.

Proceed as follows:

1. **On the File menu, select Save.**

   OR

   To save the information to a different file than a previously saved file, select Save As.

   If you are saving the configuration for the first time, the SSL VPN Cluster Manager displays the SSL VPN Cluster Manager Save window for you to select a directory and file name for storing the configuration.

   If you have saved the configuration earlier, the SSL VPN Cluster Manager updates the file selected during the first save operation with the latest configuration information.

2. **Select a folder and file name and click Save.**

Open Previously Saved Configuration

To load a previously saved configuration, proceed as follows:

1. **On the File menu, select Open.**

   The SSL VPN Cluster Manager Open window is displayed.

2. **Select the desired file and click Open.**

   If the selected file contains the configuration information in the appropriate format, the SSL VPN Cluster Manager replaces the current view of the tree with the view specified in the loaded file.

Performance Statistics

The SSL VPN Cluster Manager periodically polls the cluster's statistics to plot utilization graphs. For a better real-time presentation, the graphs are launched in a separate window and polls the statistical values on every 30 seconds. This is the default and the interval is user configurable.

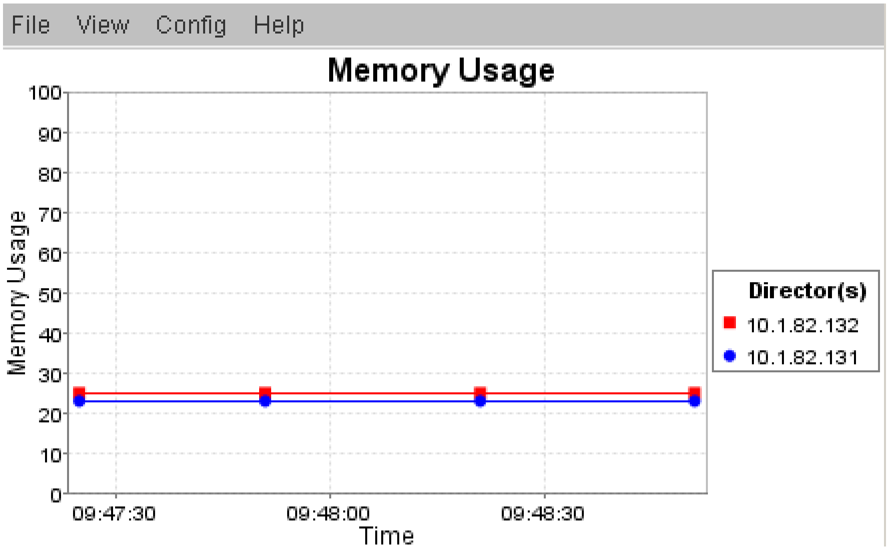
Currently, the performance graphs are available for:

- Memory Utilization
- CPU Load
- Current Sessions
- License usage

Memory Utilization

1. **In the SSL VPN Network tree view, select the desired cluster or host.**
2. **On the Tools menu, select Performance>Memory Utilization.**

   A graph is displayed.



If a cluster was selected in the SSL VPN tree view, the graph shows memory usage for all hosts included in the cluster.

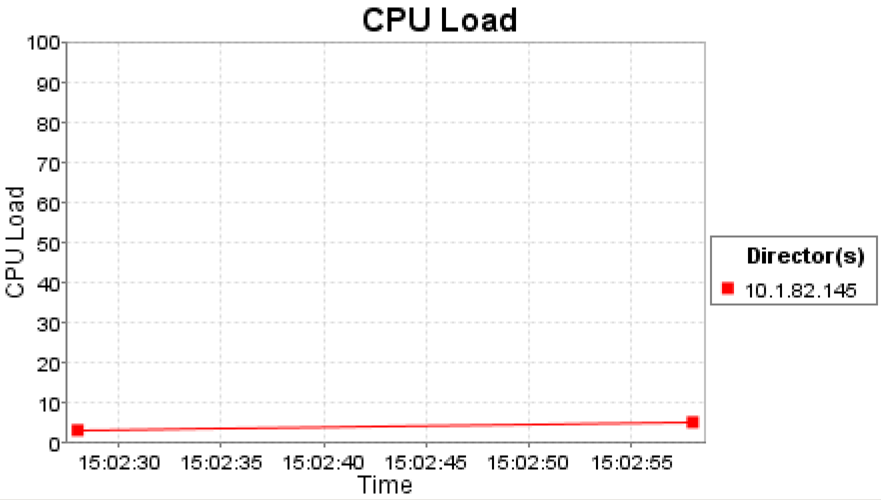
If a host was selected in the SSL VPN tree view, the graph only shows memory usage for the selected host.

CPU Load

1. **In the SSL VPN Network tree view, select the desired cluster or host.**

2. **On the Tools menu, select Performance>CPU Utilization.**

   A graph is displayed.



If a cluster was selected in the SSL VPN tree view, the graph shows CPU utilization for all hosts included in the cluster.

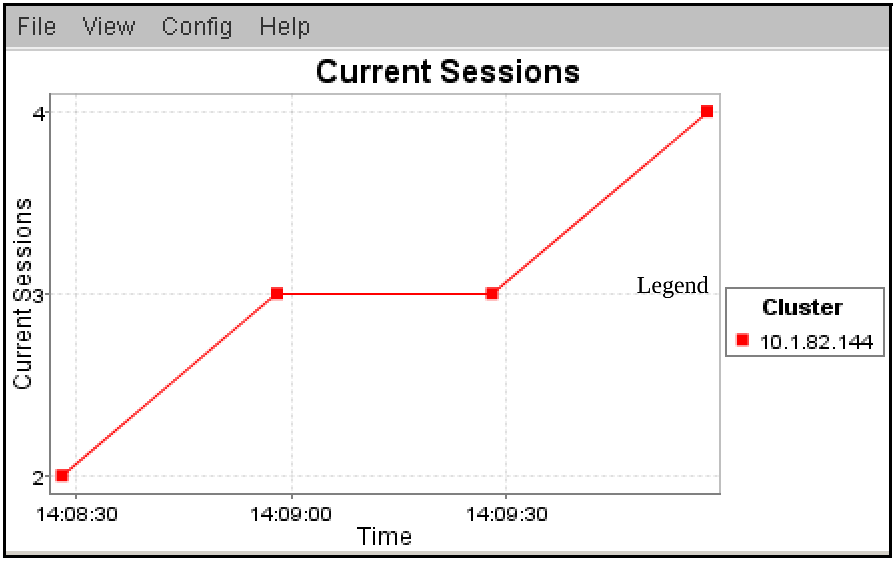
If a host was selected in the SSL VPN tree view, the graph only shows CPU utilization for the selected host.

Current Sessions

1. **In the SSL VPN Network tree view, select the desired cluster.**

2. **On the Tools menu, select Performance>Current Sessions.**

A graph is displayed.



License Usage

The following steps guide you to view the license information in graphical format:

1. **In the SSL VPN Network tree view, select the desired cluster.**

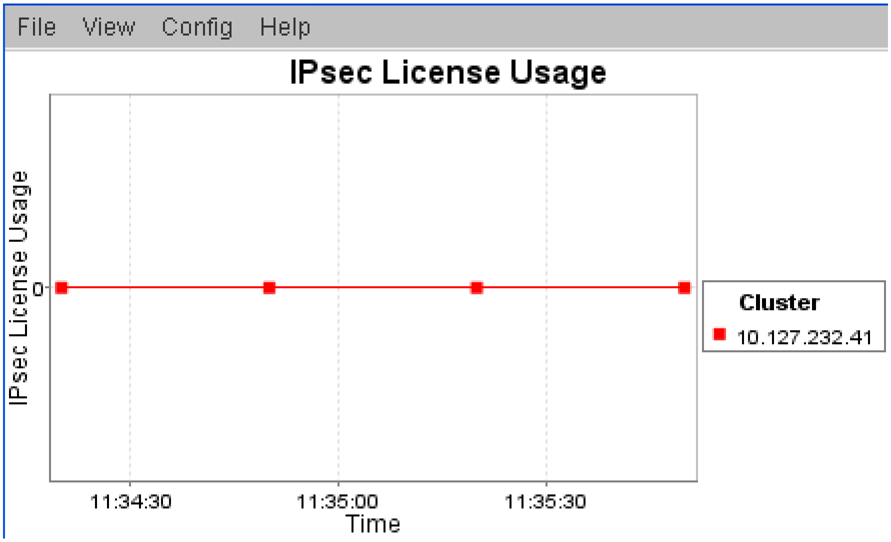
2. **On the Tools menu, select Performance>License Usage.**

   IPsec, SSL, Spike License, and All License Usage options are displayed.

NOTE – If you select All License Usage option, you can view the IPsec, SSL, and Spike License information together.

3. **Select the license usage option you wish to see. The selected option’s graph is launched.**

The following graph shows the information of IPsec License Usage.



Working with the Graphs

As long as the graph is open, it continuously accumulates statistical values polled from the hosts. The time span on the Time axis is expanded accordingly. You can zoom in and out on the desired axis or both axes

Auto Range

On the View menu, select Auto Range>Both Axes/Horizontal Axis/Vertical Axis to rescale both axes, the horizontal axis or the vertical axis so that the chart window only displays the portion of the graph that holds data.

To restore the default setting, go to the View menu and select Properties. In the Chart Properties window, select the Plot tab, the Range Axis tab and the Range tab. Finally, set Minimum range value to 0.0 and Maximum range value to 100.0.

Zoom In

On the View menu, select Zoom In>Both Axes/Horizontal Axis/Vertical Axis to zoom in on the chart.

Zoom Out

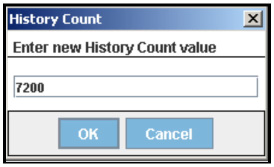
On the View menu, select Zoom Out>Both Axes/Horizontal Axis/Vertical Axis to zoom out from the chart.

History Count

If needed, you can specify a maximum number of tick values (CPU/memory data values) that should be stored by the graph. When the tick count reaches maximum value, the graph starts discarding the old values in order to store the new ones.

The default history count is set to 7200, which means that the graph can store values for 60 hours with a status polling interval set at 30 seconds (default polling interval value).

1. **On the Config menu, select History Count.**



History Count

Enter new History Count value

7200

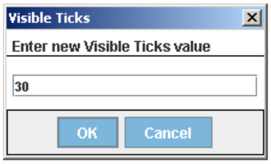
2. **Specify the desired history count value and click OK.**

Visible Ticks

The Visible Ticks count value is used to restrict the number of ticks that should be displayed on the graph. This count does not influence the number of ticks that should be stored with in the graph, it is only used for display purposes.

The default visible ticks count is set to 30. When the 31st value arrives, the 1st value is moved out to display the new data value.

1. **On the Config menu, select Visible Ticks.**



Visible Ticks

Enter new Visible Ticks value

30

2. **Specify the desired visible ticks value and click OK.**

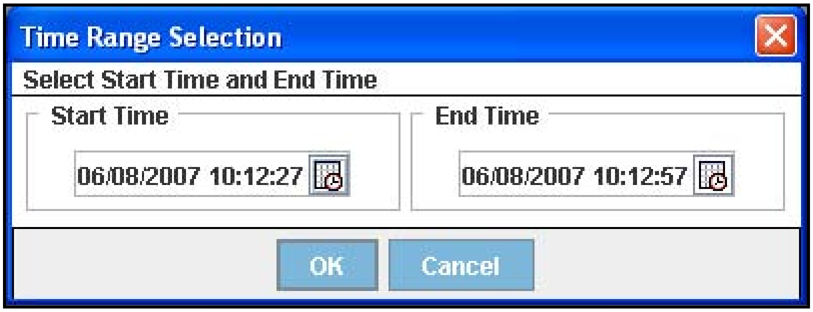
Open Customized Chart View

If desired, you can view the data moved out of the graph. The past data is shown in a separate graph for the specified time interval.

To open a new window with a customized view of the chart, proceed as follows:

1. **On the View menu, select Select.**

   The Time Range Selection window is displayed.



Time Range Selection

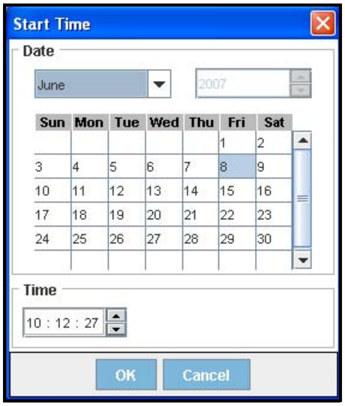
Select Start Time and End Time

Start Time: 06/08/2007 10:12:27

End Time: 06/08/2007 10:12:57

2. **Click the clock symbol in the Start Time and/or End Time areas, to select a time interval (within the current time interval) that you wish to study.**

   A calendar window is displayed.



Start Time

Date

June   2007

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Time

10 : 12 : 27

Select the desired month or year in the respective list boxes. To change the time, click on the area corresponding to hours, minutes or seconds and use the arrow buttons to change the value. It is not possible to select a value that is outside the current (accumulated) time interval.

3. **Click OK.**

   The Time Range Selection window is redisplayed.

4. **Click OK.**

   A new chart window is opened with data reflecting your selection.

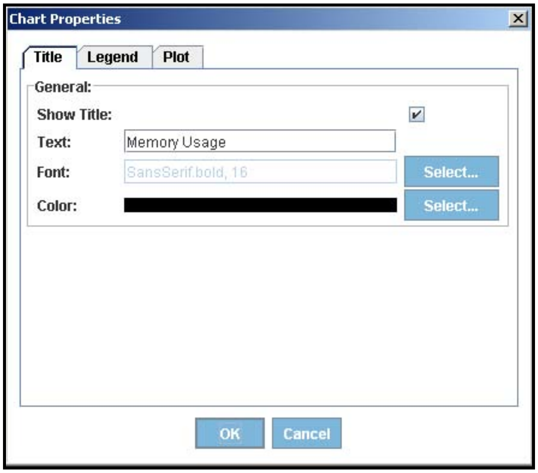
Customize the Graphs

To customize the appearance of the graph, proceed as follows:

1. **Display a graph as described previously in this section.**

2. **On the View menu, select Properties.**

   The Chart Properties window is displayed.



Show Title: ☑

Text: Memory Usage

Font: SansSerif.bold, 16

Color: ■

On the Title tab, you can change the title’s text, font and color.

The following options are available:

Show Title Deselect the check box to hide the chart title.

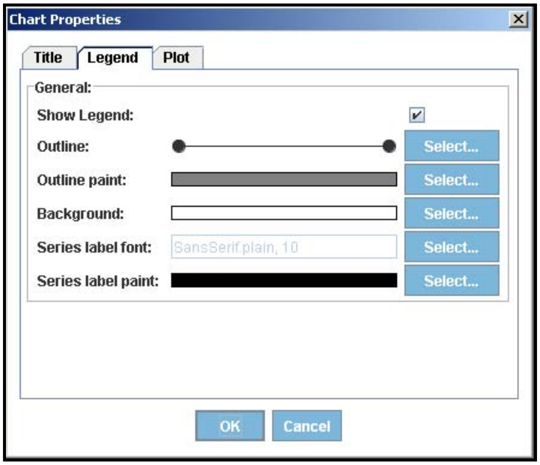
Text Enter the desired title text.

Font Click Select and select the desired font, size and attribute.

Color Click Select and select the desired color.

3. **Select the Legend tab.**

The Legend tab lets you customize the appearance of the chart’s legend.



Show Legend: ☑

Outline:

Outline paint:

Background:

Series label font: SansSerif.plain, 10

Series label paint:

The following options are available:

Show Legend — Deselect the check box to hide the legend.

Outline — Click Select and select the desired outline type and width.

Outline paint — Click Select and select the color of the outline.

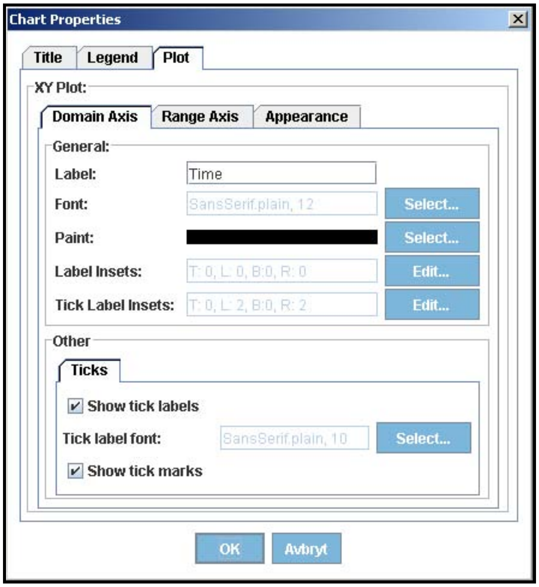
Background — Click Select and select the desired background color.

Series label font — Click Select and select the font of the legend text (not the legend title).

Series label paint — Click Select and select the color of the legend text.

4. **Select the Plot tab.**

The Plot tab lets you customize the appearance of the plot.



Label: Time

Font: SansSerif.plain, 12

Paint:

Label Insets: T: 0, L: 0, B:0, R: 0

Tick Label Insets: T: 0, L: 2, B:0, R: 2

☑ Show tick labels

Tick label font: SansSerif.plain, 10

☑ Show tick marks

The following options are available:

Domain Axis tab, General

Label
Enter the desired axis label.

Font
Click Select and select the label font, size and attribute.

Paint
Click Select and select the label color.

Label Insets
Click Edit and specify the desired insets for the axis label. For example, to create a space of approximately 1 inch (2.5 cm) from the axis to the label, enter 55 as “Top” value.

Tick Label Insets
Click Edit and specify the desired insets for the tick labels. For example, to create a space of approximately 1 inch (2.5 cm) from the axis to the tick label, enter 55 as “Top” value.

Domain Axis tab, Other

Show tick labels
Deselect to hide tick labels.

Tick label font
Click Select and select the tick label font, size and attribute.

Show tick marks
Deselect to hide tick marks.

Range Axis tab, Other, Range tab

Auto-adjust range	Rescales the vertical axis to a range that is limited to the data available at the current point of time. The axis is automatically rescaled whenever the maximum or minimum data changes.
Minimum range value	Sets the minimum value on the vertical axis, for example 0.0.
Maximum range value	Sets the maximum value on the vertical axis, for example 100.0.

Appearance tab

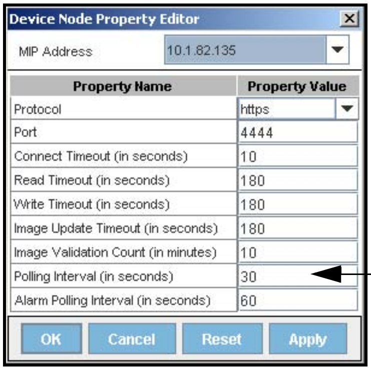
Insets	Click Edit and specify the desired insets for the whole graph. For example, to create a space of approximately 1 inch (2.5 cm) from the window’s left edge to the graph, enter 55 as “Left” value.
Outline stroke	Click Select and select the graph’s outline type and width.
Outline paint	Click Select and select the color of the graph’s outline.
Background paint	Click Select and select the background color of the graph.
Orientation	Sets the desired orientation of the graph.
Draw lines	Deselect to hide the line between the shapes in a curve.
Draw shapes	Deselect to hide the shapes (for example boxes) in a curve. Only the line will be visible.

Change Polling Interval

The graphs are updated periodically by polling the hosts at a regular time interval. The default polling interval is 30 seconds. If desired, this value can be changed in the Device Node Property Editor for the specific clusters.

1. **On the View menu and select Cluster Properties.**

   The Device Node Property Editor is displayed.



MIP Address: 10.1.82.135

Property Name	Property Value
Protocol	https
Port	4444
Connect Timeout (in seconds)	10
Read Timeout (in seconds)	180
Write Timeout (in seconds)	180
Image Update Timeout (in seconds)	180
Image Validation Count (in minutes)	10
Polling Interval (in seconds)	30
Alarm Polling Interval (in seconds)	60

Polling interval

2. **On the Polling Interval row, in the Property Value column, enter the desired value.**

3. **Click OK.**

Save Graph

A graph can be saved and opened later. When viewing a previously saved graph, all the options that are available for a "live" graph will be also be available for the saved graph, for example zooming in and out, selecting a time interval and customizing the graph's properties.

1. **Display the desired graph as described previously in this section.**

2. **On the File menu, select Save Data.**

3. **Save the file to the desired folder.**

Open Graph

1. **In the Cluster Manager's main window, on the Tools menu, select Open Graph.**

2. **Navigate to the folder where you saved the file and open it.**

Display Cluster Alarms

Using this function, alarms generated by all the clusters in the SSL VPN Network tree view can be viewed.

View Alarms for All Clusters

To view alarms of all the clusters, proceed as follows:

1. **On the Tools menu, select Alarms>Alarms Of All Clusters.**

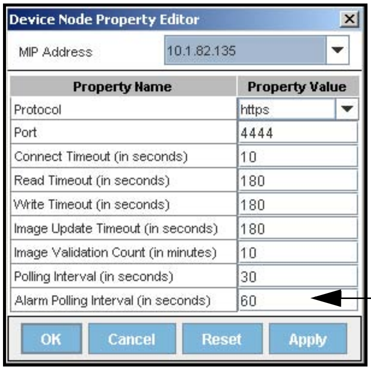
The Alarms On All Devices window is displayed.

The window shows alarms generated by all clusters in the SSL VPN Network tree, in a tabular format.

The Severity column values are displayed in red color for major/critical alarms. The table columns can be sorted either in ascending/descending order by selecting particular column header.

The table is updated periodically by polling all the clusters at a regular time interval. The default alarm polling interval is 60 seconds. If desired, this value can be changed in the Device Node Property Editor for the specific clusters.

To display the Device Node Property Editor, go to the View menu and select Cluster Properties.



Device Node Property Editor

MIP Address: 10.1.82.135

Property Name	Property Value
Protocol	https
Port	4444
Connect Timeout (in seconds)	10
Read Timeout (in seconds)	180
Write Timeout (in seconds)	180
Image Update Timeout (in seconds)	180
Image Validation Count (in minutes)	10
Polling Interval (in seconds)	30
Alarm Polling Interval (in seconds)	60

Alarm polling interval

View Alarms for Specific Cluster

1. **In the SSL VPN Network tree view, select the desired cluster.**
2. **On the Tools menu, select Alarms>Alarms Of <cluster IP address>.**

The Alarms On <cluster IP address> window is displayed.

For a total listing of possible alarms, see the Appendix C, “Syslog Messages” in the *User’s Guide*.

Display License Information

Using this function, license usage information can be viewed.

Viewing license information in Excel format

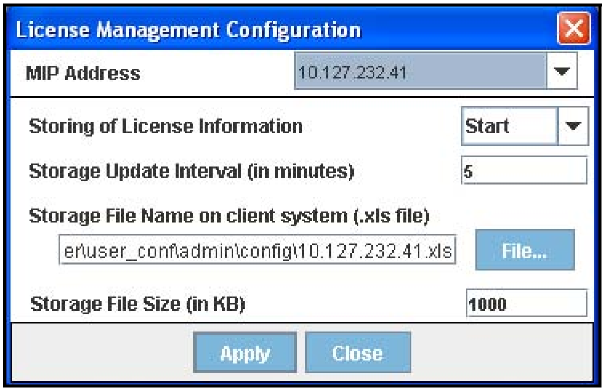
The following steps guide you to view the license information in Excel format:

1. **Select Tools > License Management Configuration.**

   License Configuration window is displayed.

2. **Specify the following parameters:**

   - Enable/disable storage of the license information in Excel format
   - Interval to be used to update the license information
   - Name of the Excel file
   - File size



License Management Configuration

MIP Address: 10.127.232.41

Storing of License Information: Start

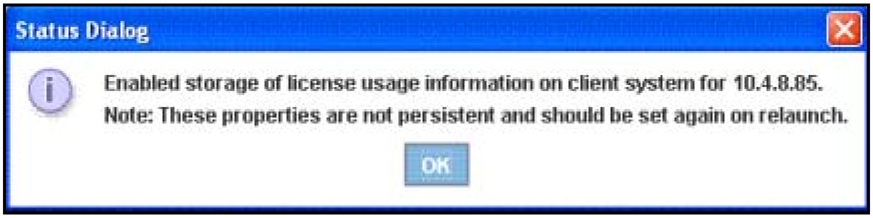
Storage Update Interval (in minutes): 5

Storage File Name on client system (.xls file): er\user_conf\admin\config\10.127.232.41.xls

Storage File Size (in KB): 1000

3. **Click Apply**

The Status Dialog message is displayed.



Enabled storage of license usage information on client system for 10.4.8.85.
Note: These properties are not persistent and should be set again on relaunch.

4. **Click Close.**
5. **Navigate to the folder where you saved the file and click Open.**

APPENDIX A

Virtual Desktop

This Appendix provides ongoing support for the virtual desktop.

Virtual Desktop is a Java application that provides protection against lost or theft of sensitive information. Files created while in the virtual desktop are encrypted as they are saved to a hard drive or removable media. Integrating Virtual Desktop with AVG will provide a secure environment for end users while accessing confidential information.

The virtual desktop licenses are available in volumes of 50, 100, 250, 500, 1000, 2000, and 5000.

Starting Vdesktop

Integrated Virtual Desktop is started under the following scenarios:

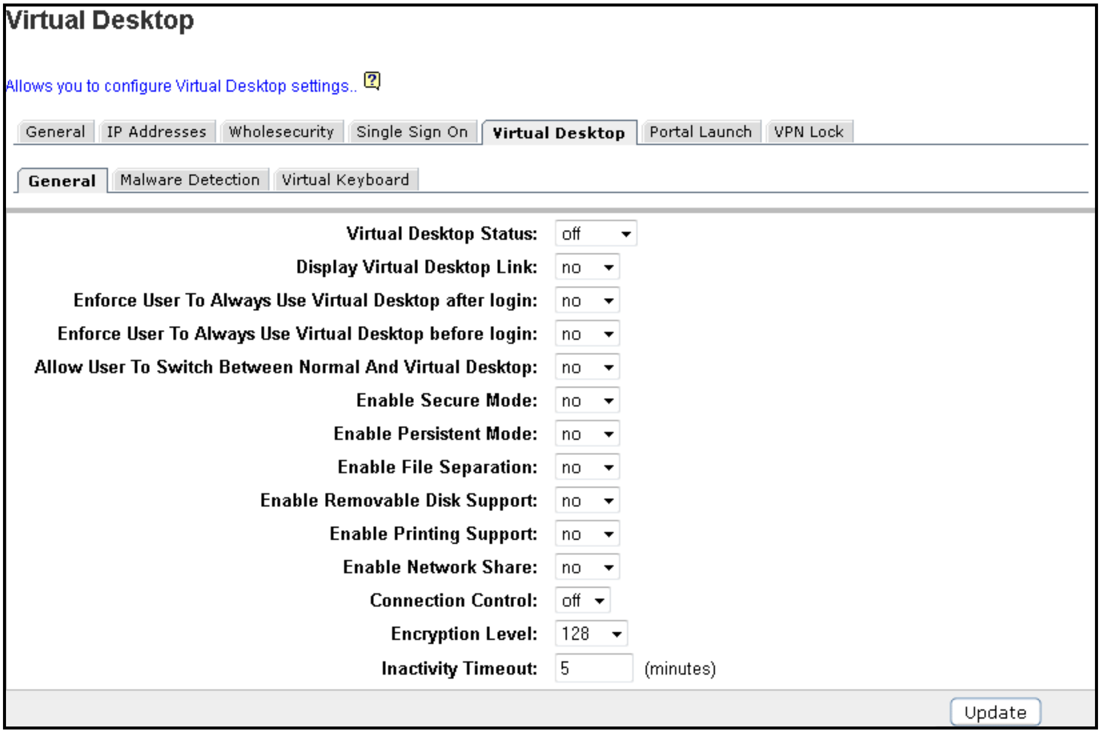
- Pre-logon: Users can launch Virtual Desktop before logging on. An additional link will be displayed on the Login page to start Virtual Desktop.
- Always: User session is moved to virtual desktop, upon successful login. Current user session cookies are migrated to the virtual desktop session so that the user does not have to authenticate again. Portal session outside the virtual desktop will be closed.
- Force: Users will be forced to always login from within the Virtual Desktop. On navigating to the portal login page, virtual desktop will be launched. Portal login page will be loaded inside Virtual Desktop. This is a per VPN setting.
- "Virtual Desktop" Avaya Endpoint Access Control Agent rule: Users will be forced to use the Virtual Desktop, if the Avaya Endpoint Access Control Agent check for host integrity fails (firewall, virus scanner and so on). The session outside the Virtual Desktop will be closed.

Configure General Settings for Vdesktop

This section explains the steps to configure the general settings for Virtual Desktop for the current VPN.

1. **Logon as system administrator.**
2. **Click on Config tab.**
3. **In system tree view select VPN Gateways.**
4. **Select the name of the VPN Gateway.**
5. **Under Settings, select General.**
6. **Click on vdesktop tab.**

   Virtual Desktop screen is displayed.



Virtual Desktop

Allows you to configure Virtual Desktop settings..

Virtual Desktop Status:	off
Display Virtual Desktop Link:	no
Enforce User To Always Use Virtual Desktop after login:	no
Enforce User To Always Use Virtual Desktop before login:	no
Allow User To Switch Between Normal And Virtual Desktop:	no
Enable Secure Mode:	no
Enable Persistent Mode:	no
Enable File Separation:	no
Enable Removable Disk Support:	no
Enable Printing Support:	no
Enable Network Share:	no
Connection Control:	off
Encryption Level:	128
Inactivity Timeout:	5 (minutes)

7. **Specify whether to enable or disable Virtual Desktop.**
8. **Specify whether to show virtual desktop link on the login page or not.**

9. **Specify whether to force the user to use virtual desktop after login or not.**

10. **Specify whether to force the user to use virtual desktop before login.**

11. **Set this option to 'on' to allow switching between regular and virtual desktops.**

12. **Set this option to force the user into the browser and to forbid any other program usage within the Virtual Desktop (with the exception of executables required to enable malicious code prevention features).**

13. **Enable persistent mode to allow users access to Persistent Desktop data offline.**

    When the Virtual Desktop module exits, the link and relevant data files are kept on the endpoint system. After the Virtual Desktop module has exited, Persistent Desktop link is added to the Start menu. Users can click this link to start the Virtual Desktop module offline. Users can also choose to exit the Persistent Desktop and remove all data. If the Persistent Desktop option is not enabled, the Virtual Desktop content is automatically destroyed at the end of the Virtual Desktop session.

14. **Set this option to prevent users from seeing or using the files that are on the normal desktop.**

    - When it is enabled, all folders and files on the normal desktop are hidden, with the exception of system files. Only the Documents and Settings, Program Files and Windows folders, and their contents are visible.
    - When it is disabled, then all files on the normal desktop are virtualized and thus visible and accessible within the Virtual Desktop.

15. **Set this option to save files to a removable disk.**

    - When it is enabled, it permits the users to copy files from the Virtual Desktop to a floppy disk, USB flash drive, or other removable storage that is attached to the client computer.
    - When it is disabled, users will essentially have a terminal session, and will not be able to save any files or other data from their sessions.

16. **Set this option to permit the users to print files from the Virtual Desktop.**

    - When it is enabled, it permits the users to print files from the Virtual Desktop.
    - When it is disabled, users will not be able to print files or other data from their sessions.

NOTE – Adobe PDF Writer uses the same spool used by the printer when generating PDF files, users cannot create PDF files from within the Virtual Desktop when this option is enabled.

17. **Set this option to permit the users to save files and map drives from the Virtual Desktop through Windows SMB.**

    - When it is enabled, the Virtual Desktop allows users from copying files to a drive that is already mapped in the regular desktop, and allows users from copying data to a mapped drive from the command prompt.
    - When it is disabled, the Virtual Desktop prevents users from copying files to a drive that is already mapped in the regular desktop, and prevents users from copying data to a mapped drive from the command prompt.

18. **Set encryption level for virtual desktop.**

    The default is 128-bit RC4 encryption, but you can choose 128-bit, 512-bit, or 1024-bit encryption. This is the level of protection that is applied to the data that is on the Virtual Desktop.

19. **Set this option to configure inactivity timeout for virtual desktop in minutes.**

    At the end of the timeout period, the application closes and the Virtual Desktop or Cache is wiped clean.

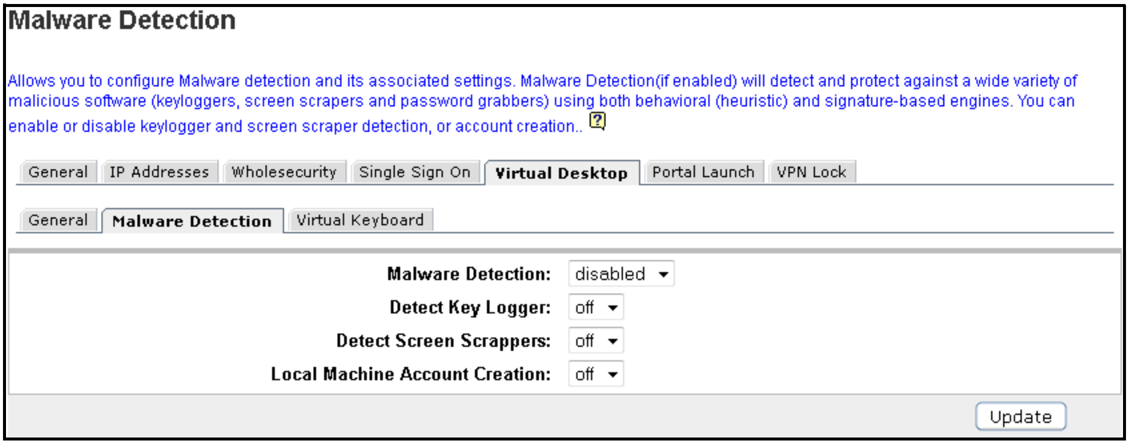
20. **Click Update to submit the specified Virtual Desktop Settings to the pending configuration.**

    Once the portal is launched from the Virtual Desktop, Avaya Endpoint Access Control Agent will try to verify the rules for the group. “Virtual Desktop” TG rule essentially checks whether the browser session is running from within the Virtual Desktop. To verify this TG will use the platform dll to check the parent process of the current browser instance. If the parent process is virtual desktop, the rule will pass and proceed to display portal content.

Configure Malware Detection Settings

This section explains the steps to configure malware detection settings associated with the currently selected VPN.

1. **Logon as system administrator.**
2. **Click on Config tab.**
3. **In system tree view select VPN Gateways.**
4. **Select the name of the VPN Gateway.**
5. **Under Settings, select General.**
6. **Click Malware Detection tab.**



Malware Detection

Allows you to configure Malware detection and its associated settings. Malware Detection(if enabled) will detect and protect against a wide variety of malicious software (keyloggers, screen scrapers and password grabbers) using both behavioral (heuristic) and signature-based engines. You can enable or disable keylogger and screen scraper detection, or account creation..

Malware Detection: disabled

Detect Key Logger: off

Detect Screen Scrappers: off

Local Machine Account Creation: off

7. **Enable Malware Detection.**
8. **Enable the detection of key loggers.**

   Therefore this monitors every key stroke a user types on the key board. The default value is disabled (off).

9. **Enable the detection of screen scrappers or not.**

   Screen scrappers usually ignores the binary data and formatting that makes the desired text less visible. The default value is off.

10. **Enable the prevention of creating local accounts.**

    The default value is off.

11. **Click Update.**

Configuring Virtual Keyboard

You can configure the MCD (Malware Detection) with the Virtual Keyboard to invoke the Virtual Keyboard in the event that malware is detected. This can be used to protect against keystroke loggers during login and during the VPN session.

After the integration, if a personal computer (PC) is infected, MCD detects the infection and does not allow the PC to logon. Based on the configuration settings, the integration forces the PC to the virtual desktop or keyboard. The integration also upgrades Symantec On Demand Protection (SODP) to version 3.1 and consolidates the SODP Agent files used by the SPO and Portal to one location.

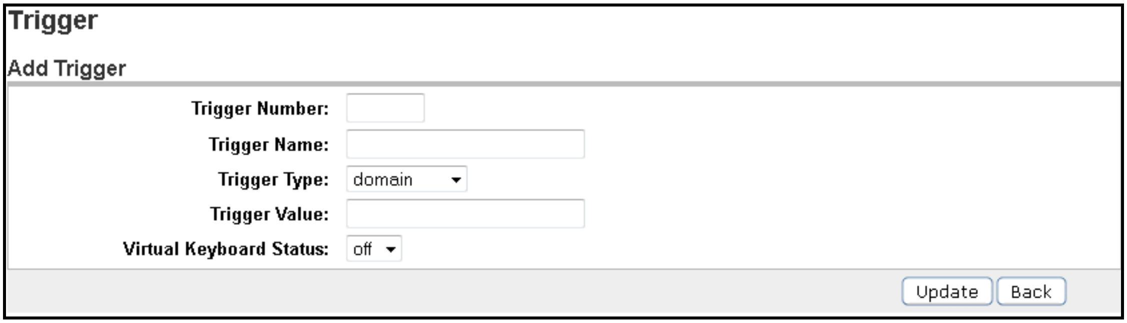
To configure the Virtual Keyboard, perform the following procedure:

1. **Logon as the system administrator.**
2. **Click the Config tab.**
3. **In system tree view, select VPN Gateways.**
4. **Select the name of the VPN Gateway.**
5. **From Settings, select General.**
6. **Click the Virtual Keyboard tab.**
7. **Click the General tab.**
8. **From the Virtual Keyboard Status list, select enabled.**
9. **Click Update.**

   The Virtual Keyboard is enabled.

10. **Click the Trigger tab.**
11. **Click Add.**

The Add Trigger form appears.



Trigger

Add Trigger

Trigger Number:	
Trigger Name:	
Trigger Type:	domain
Trigger Value:	
Virtual Keyboard Status:	off

12. **In the Trigger Number field, enter the trigger number.**
13. **In the Trigger Name field, enter the trigger name.**
14. **From the Trigger Type list, select the trigger type.**
15. **In the Trigger Value field, enter the trigger value.**
16. **From the Virtual Keyboard Status list, select on.**
17. **Click Update.**

    The trigger is added.

18. **Apply the changes.**

Glossary

Access Rules

When a user tries to log in to the VPN, either through the Portal page or through a VPN client, his or her group membership determines the access rights to different servers and applications on the intranet. This is done by associating one or more access rules (each containing parameters such as allowed network, ports and paths) with a group.

ARP

Address Resolution Protocol. A network layer protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

Avaya Endpoint Access Control Agent

Avaya Endpoint Access Control Agent is an application that checks that the required components (executables, DLLs, configuration files, etc.) are installed and active on the remote user’s machine.

Base Profile

Refers to links and access rules specified for a user group directly under the Group level. If extended profiles are used, the base profile’s links and access rules will be appended to the extended profile’s links and access rules.

Branch Office Tunnel

Secure IPsec tunnel between two Avaya VPN Gateways (or cluster of Avaya VPN Gateways) or similar devices. The tunnel is automatically established when traffic destined for specific remote networks is detected, provided traffic was initiated from a network allowed to send traffic through the tunnel. BO tunnels can e.g. be set up between a main office and a branch office.

BWM (Bandwidth Management)

Enables Web site managers to allocate a portion of the available bandwidth for specific users or applications. You can configure BWM policies to set lower and upper bounds on the bandwidth allocation.

CA (Certificate Authority)

A trusted third-party organization or company that issues digital certificates. The role of the CA in this process is to guarantee that the entity granted the unique certificate is, in fact, who he or she claims to be.

CLI (Command Line Interface)

The text-based interface on the Avaya VPN Gateway, presented to the user after having logged in. The CLI can be accessed through a console connection or remote connection (Telnet or SSH). The CLI is used for collecting information and configuring the Avaya VPN Gateway.

Cluster (of Avaya VPN Gateways)

A cluster is a group of Avaya VPN Gateways that share the same configuration parameters. There can be more than one Avaya VPN Gateway cluster in the network, each with its own set of parameters and services to be used with different real servers. Every cluster has a Management IP address (MIP), which is an IP alias to one of the master Avaya VPN Gateways in the cluster.

Console Connection

A connection to the Avaya VPN Gateway established through the console port.

CRL (Certificate Revocation List)

A list containing the serial numbers of revoked client certificates. Each CA issues and maintains their own CRLs. If you generate client certificates on the Avaya VPN Gateway, you can also create your own CRL.

CSR (Certificate Signing Request)

A request for a digital certificate, sent to a CA. On the Avaya VPN Gateway, you can generate a CSR from the command line interface by using the `request` command.

DCE (Data Communication Equipment)

A device that communicates with a Data Terminal Equipment (DTE) in RS-232C communications.

DER (Distinguished Encoding Rules)

A process for unambiguously converting an object specified in ASN.1 (such as an X.509 certificate, for example) into binary values for storage or transmission on a network.

Digital Certificate

The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by trusted third parties known as certificate authorities (CAs), after verifying that a public key belongs to a certain owner. The certification process varies depending on the CA and the level of certification.

Digital Signature

A digital guarantee that a document has not been altered, as if it were carried in an electronically-sealed envelope. The “signature” is an encrypted digest of the text that is sent with the text message. The recipient decrypts the signature digest and also recomputes the digest from the received text. If the digests match, the message is proved intact and tamper free from the sender.

A digital signature ensures that the document originated with the person signing it and that it was not tampered with after the signature was applied. However, the sender could still be an impersonator and not the person he or she claims to be. To verify that the message was indeed sent by the person claiming to send it requires a digital certificate (digital ID) which is issued by a certification authority.

DIP (Destination IP) Address

The destination IP address of a frame.

DPort (Destination Port)

The destination port number, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.

DTE (Data Terminal Equipment)

A device that controls data flowing to or from a computer. The term is most often used in reference to serial communications defined by the RS-232C standard. This standard defines the two ends of the communication channel as being a DTE and DCE device. However, using a null-modem cable, a DTE to DTE communication channel can also be established between, for example, two computers.

Extended Profile

Extended profiles can be defined for a user group if other links and access rules should apply when the user authenticates by means of a specific authentication method or when connecting from a specific IP address or network.

HTTP Proxy

Java applet accessible on the Portal page’s Advanced tab, enabling links executed on complex intranet Web pages (containing plugins like Flash, Shockwave and Java applets) to be sent through a secure connection to the SSL server for redirection.

L2TP (Layer 2 Tunneling Protocol)

Acts as a data link layer protocol for tunneling network traffic between two peers over an existing network or Internet.

Master

An Avaya VPN Gateway in a cluster that is in control of the MIP address, or can take over the control of the MIP address should another master fail. Configuration changes in the cluster are propagated to other members through the master Avaya VPN Gateways.

MIB (Management Information Base)

An SNMP structure that describes which groups and objects that can be monitored on a particular device.

MIP (Management IP) Address

An IP address that is an IP alias to a master Avaya VPN Gateway in a cluster of Avaya VPN Gateways. The MIP address identifies the cluster and is used when making configuration changes through a Telnet or SSH connection or through the Browser-Based Management Interface (BBI).

NAP (Network Access Protection)

Provides system health validation access to the private networks. The NAP provides an integrated way of validating the health state of a network client attempting to connect or communicate on a network.

Net Direct Client

The Net Direct client is an SSL VPN client that can be downloaded from the Portal for each user session. As opposed to the LSP and TDI versions of the Avaya VPN Client, the Net Direct client does not have a user interface. Another difference is that the Net Direct client is packet-based, while the Avaya VPN Client uses system calls. The packet-based solution supports more applications (e.g. Microsoft Outlook).

Nslookup

A utility used to find the IP address or host name of a machine on a network. To use the `nslookup` command on the Avaya VPN Gateway, it must have been configured to use a DNS server.

NTP (Network Time Protocol)

A protocol used to synchronize the real-time clock in a computer. There are numerous primary and secondary servers on the Internet that are synchronized to the Coordinated Universal Time (UTC) through radio, satellite or modem.

AVG

Avaya VPN Gateway.

Passphrase

Passphrases differ from passwords only in length. Passwords are usually short, from six to ten characters. Short passwords may be adequate for logging onto computer systems that are programmed to detect a large number of incorrect guesses, but they are not safe for use with encryption systems. Passphrases are usually much longer—up to 100 characters or more. Their greater length makes passphrases more secure.

PEM (Privacy Enhanced Mail)

A standard for secure e-mail on the Internet. It supports encryption, digital signatures and digital certificates as well as both private and public key methods. Keys and certificates are often stored in the PEM format.

Ping (Packet INternet Groper)

A utility used to determine whether a particular IP address is online.

PKCS #12

A standard for storing private keys and certificates.

PKI (public key infrastructure)

Short for *public key infrastructure*, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread.

A PKI is also called a *trust hierarchy.*

Portal

The Portal web page is displayed following a successful login to a VPN server of the portal type. The Portal contains different tabs from where the user can access various intranet resources such as web, mail and file servers.

Portal Guard

The Portal Guard feature is an easy way of “converting” an existing HTTP site to generate HTTPS links, secure cookies etc. The Avaya VPN Gateway will not only handle the SSL processing but also see to it that all existing web links are rewritten to HTTPS. This eliminates the need to rewrite each link manually.

Port Forwarder

Java applet accessible on the Portal page’s Advanced tab, enabling transparent access to applications through a secure connection. By specifying an arbitrary port number on the client along with the desired intranet host and port number, the user can access an intranet application by connecting to localhost on the specified port number.

Secure Service Partitioning

Feature designed to partition a cluster of Avaya VPN Gateways into separate VPNs. The idea is to give service providers (ISPs) the possibility to host multiple VPN customers on a shared Remote Access Services (RAS) platform.

Setup Utility

When turning on an Avaya VPN Gateway the very first time, the Setup utility starts up automatically. The Setup utility is used for performing a basic configuration of the Avaya VPN Gateway. The Setup utility first presents you with the choice of setting up the Avaya VPN Gateway as a single device, or to add the Avaya VPN Gateway to an existing cluster.

If you perform a reinstallation of the Avaya VPN Gateway software, you will also enter the Setup Utility after the Avaya VPN Gateway has rebooted.

SIP (Source IP) Address

The source IP address of a frame.

Slave

An Avaya VPN Gateway that depends on a master Avaya VPN Gateway in the same cluster for proper configuration.

SNMP (Simple Network Management Protocol)

A network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (an Avaya VPN Gateway, for example), to the workstation console (or SNMP manager) used to oversee the network. The SNMP agents return information contained in a MIB (Management Information Base), which is a data structure that defines what information is obtainable from the device.

SOCKS

A generic, proxy protocol for TCP/IP-based networking applications. The SOCKS protocol provides a flexible framework for developing secure communications by easily integrating other security technologies, e.g. SSL.

SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS server, without requiring direct IP reachability.

Spike

A Spike license provides remote access in a secure way.

SPort (Source Port)

The source destination port, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.

SPO (Secure Potable Office)

The SPO client provides VPN access from portable storage such as USB compliant flash memory and CD ROM.

The SPO client provides enhanced mobility, portability, and security compared to traditional VPN access methods. The SPO client can be deployed and managed from the AVG server thus simplifying SPO client maintenance and updates.

SSH (Secure Shell)

A program used to log into another computer over a network, execute commands in a remote machine, and move files from one machine to another. SSH provides strong authentication and secure communications over insecure channels.

SSL (Secure Sockets Layer) Protocol

The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and following higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.

SSL VPN Client

Windows application with SOCKS support. When installed on a user’s computer, transparent access (not through the Portal page) to intranet applications is enabled.

TLS (Transport Layer Security)

The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Traceroute

A utility used to identify the route used for station-to-station connectivity across the network.

Trap

If a trap is defined in the MIB, a trap message is sent from the SNMP agent to the SNMP manager when the trap is triggered. A trap can for example define a hardware failure in a monitored device.

URI (Uniform Resource Identifier)

The addressing technology from which URLs are created. Technically, URLs such as HTTP:// and FTP:// are specific subsets of URIs, although the term URL is mostly heard.

Virtual Desktop (Vdesk)

Virtual Desktop is a Java application that provides protection against lost or theft of sensitive information.

VIP (Virtual IP) Address

An IP address that the remote user should connect to access Portal/VPN (in clientless mode) or simply the VPN (in transparent mode).

Virtual SSL Server

A virtual SSL server handles a specific service on the Avaya VPN Gateway, such as HTTPS, SMTPS, IMAPS, or POP3S. You can create up to 256 virtual SSL servers per Avaya VPN Gateway cluster. To authenticate itself towards clients making requests for the specified service, the virtual SSL server is configured to use a digital certificate.

VLAN (Virtual Local Area Network)

VLANs are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.

X.509

A widely-used specification for digital certificates that has been a recommendation of the ITU since 1988.

X11 Forwarding

The X Window System (commonly X11 or X) is a windowing system for bitmap displays. It is the standard toolkit and protocol to build graphical user interfaces on Unix, Unix-like operating systems and OpenVMS, and is available for almost all modern operating systems. The Avaya VPN Gateway supports secure display of X11 across the Internet by way of X11 Forwarding, supported by the SSH applet on the Portal’s Advanced tab and the Terminal link type.