Command Reference
Avaya VPN Gateway

Release 9.0
NN46120-103
Issue 04.03
April 2013

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 websites referenced within this site or documentation 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 its hardware and Software (“Product(s)”). 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 website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and

design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation 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 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

This Guide lists all the CLI commands available in the Avaya VPN Gateway (AVG) software. The software supports both SSL Acceleration and VPN.

Who Should Use This Book

This Guide is for network installers and system administrators who configures and maintains a network. You must be familiar with Ethernet concepts and IP addressing.

Related documentation

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

- *Avaya VPN Gateway Command Reference* (NN46120-103). Describes each command in detail. The commands are listed for each menu, according to the order they appear in the Command Line Interface (CLI).
- *Avaya VPN Gateway Application Guide for SSL Acceleration* (NN46120-100). Provides examples on how to configure Secure Socket Layer (SSL) Acceleration through the CLI.
- *Avaya VPN Gateway CLI Application Guide* (NN46120-101). Provides examples on how to configure VPN deployment through the CLI.
- *Avaya VPN Gateway BBI Application Guide* (NN46120-102). Provides examples on how to configure VPN deployment through the Browser-Based Interface (BBI).
- *Avaya VPN Gateway User Guide* (NN46120-104). Describes the initial setup procedure, upgrades, operator user management, certificate management, troubleshooting and other general operations that apply to both SSL Acceleration and VPN.
- *Avaya VPN Gateway Administrator Guide* (NN46120-105). VPN management guide intended for end-customers in a Secure Service Partitioning configuration.
- *Avaya VPN Gateway Configuration - Secure Portable Office Client* (NN46120-301). Gives the feature list and provides general information about Secure Portable Office (SPO) based VPN client.
- *Avaya VPN Gateway VMware Getting Started Guide* (NN46120–302). Describes how to install, configure, and deploy the Avaya VPN Gateway VMware appliances.

- *Avaya VPN Gateway Release Notes* (NN46120-400). Lists new features available in version and provides up-to-date product information.
- *Avaya VPN Gateway Troubleshooting Guide* (NN46120-700). Describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway (AVG).

Product Names

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

- Avaya VPN Gateway 3050-VM.
- Avaya VPN Gateway 3070-VM.
- Avaya VPN Gateway 3090-VM.

Similarly, all references to the old product name iSD-SSL or iSD in commands or system feedback are interpreted as applying to the preceding hardware models.

Note:

Manufacturing of the SSL Accelerator (formerly Alteon SSL Accelerator) has been discontinued.

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.

- Getting technical documentation on page 14
- Getting product training on page 15
- Getting help from a distributor or reseller on page 15
- Getting technical support from the Avaya Web site on page 15

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.

Chapter 2: New in this release

The following sections detail what's new in *Avaya VPN Gateway Command Reference* (NN46120-103) for Release 9.0.

Features

See the following sections for information about feature changes:

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.

Android L2TP/IPsec support

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

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

AES 256 support for IPsec

Release 9.0.0 adds AES 256 support for IPsec.

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

- cfg vpn id l2tp ikeprof id enc IKE Profile Encryption on page 278
- cfg vpn id l2tp ikeprof id dh Diffie-Hellman Group Configuration on page 279
- cfg vpn id ipsec ikeprof id enc IKE Profile Encryption on page 289
- cfg vpn id ipsec ikeprof id dh Diffie-Hellman Group Configuration on page 290

Java RDP upgrade support

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

Net Direct Mac OS X support

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

Secure Portable Office (SPO) support

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

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

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

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

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

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

Other changes

The following are changes that are not feature-related:

- Please note, while the Avaya Endpoint Access Control Agent (formerly Tunnel Guard) can be configured through both the BBI and CLI, the CLI configuration is performed under the former Tunnel Guard context.
- Added Initial Contact Payload command to L2TP tunneling, cfg vpn id l2tp ikeprof id icp Initial Contact Payload Configuration on page 281

Chapter 3: Command Reference

This chapter describes how to use the Command Line Interface (CLI) on the Avaya VPN Gateway (AVG). The chapter explains of all available commands.

Menu Basics

You can use the Command Line Interface (CLI) to view information and statistics. In addition, the administrator can use the CLI for configuring all levels of the VPN Gateway.

The various CLI commands are grouped into a series of menus and submenus. Each menu displays a list of commands and/or submenus that are available, along with a summary of the purpose of each command. Below each menu is a prompt where you can enter any command appropriate to the current menu.

When you create new CLI objects (for example, a new interface or a new group), you start a wizard that provides the relevant questions for that object. The regular menu for the object appears after the wizard closes.

This section describes the Main menu commands and provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

Global Commands

Some basic commands are recognized throughout the menu hierarchy. These commands are useful to obtain online help, to navigate through menus, and for apply and save configuration changes.

Table 1: Global Commands

Command	Action
help	Display a summary of the global commands.
help <*command*>	Display help for a specific command in the command line interface. Example: Type the /cfg/sys command at any prompt in the CLI to display the System menu. Achieve the same result by only typing /cfg/sys (no quotation marks) at any menu prompt.
.	Display the current menu.

Command	Action
print	Display the current menu.
..	Go up one level in the menu structure.
up	Go up one level in the menu structure.
/	Place at the beginning of a command to go to the Main menu. Otherwise, this is used to separate multiple commands placed on the same line.
cd " <*menu/path*> "	Display the menu indicated within quotation marks. Example: Type **cd /cfg/sys** at any prompt in the CLI to display the System menu. The same result is achieved by only typing **/cfg/sys** (no quotation marks) at any menu prompt.
pwd	Display the command path used to reach the current menu.
apply	Apply pending configuration changes.
diff	Show any pending configuration changes. Passwords and secrets (if any) are displayed as (SECRET).
revert	Remove pending configuration changes between **apply** commands. Use this command to restore configuration parameters set since the last **apply** command.
paste	Restore a previously dumped configuration. Before pasting the configuration, Provide the password phrase you specified when you ran the dump command. For more information, see the **dump** command.
exit	Terminate the current session and log out. If you have unapplied (pending) configuration changes when using the **exit** command, you are notified. If you choose to log out anyhow without using the apply command, your pending configuration changes are lost.
quit	Same as Exit. If you have unapplied (pending) configuration changes when using the **quit** command, you are notified. If you choose to log out without using the apply command, your pending configuration changes are lost.
CTRL+^	Exit from the command line interface in case the VPN Gateway stops responding. Use this command only when you connect to a specific VPN Gateway through a console connection, not when you connect to the Management IP of the cluster through a Telnet or SSH connection.
netstat	Show the current network status of the VPN Gateway. The netstat command provides information about active TCP

Command	Action
	connections, as well as the state of all TCP/IP servers and the sockets used by them.
nslookup	Find the IP address or host name of a machine. To use this command, you must configure the VPN Gateway to use a DNS server. Example: >> Configuration# nslookup Enter Hostname | IpAddress: 47.80.21.24; Server: zsc4s011.us.avaya.com ; Address: 47.81.2.10
ping	Verify station-to-station connectivity across the network. The format is as follows: **ping** <*IP address or host name*> The DNS parameters must be configured to specify host names (see /cfg/vpn <id> /adv/dns/servers DNS Servers Configuration).
traceroute	Identify the route used for station-to-station connectivity across the network. The format is as follows: **traceroute** <*IP address or host name of target station*> As with **ping,** the DNS parameters must be configured if specifying host names.
cur	View all the current settings for the active menu. Passwords and secrets (if any) are displayed as (SECRET).
curb	Brief version of the current settings for the active menu.
dump	Dump the current configuration for the active menu. You can cut and paste the dumped information in to another operator's CLI at the same menu level. The **dump** command is also available in all statistics menus to display statistics information for the active menu. When you use the **dump** command, no secret value is dumped unless a dump password is given, and the secret value is encrypted. Use the **paste** command to dump. The password provided by the **dump** command should be supplied.
lines *n*	Set the number of lines (*n*) to appear on the screen at one time. The default value is 24 lines. When used without a value, the current setting appears.
verbose *n*	Configures the level of information displayed on the screen: 0 = Quiet: Nothing appears except errors—not even prompts. 1 = Normal: Prompts and requested output are shown, but no menus. 2 = Verbose: Everything is shown. The default level is 2. When used without a value, the current setting appears.
slist	Displays a list of all Admin user sessions currently running in the cluster.

CommandLine History and Editing

Using the command line interface, you can retrieve and modify previously entered commands with a few keystrokes. The following options are available globally at the command line.

Table 2: Command Line History and Editing Options

Option	Description
history	Display a numbered list of the last 10 previously entered commands.
!!	Repeat the last entered command.
! *n*	Repeat the *n* th command on the history list.
pushd	"Bookmarks" your current position in the menu structure. After moving to another level or command in the menu structure, you can easily return to the bookmarked position by typing the **popd** command. Combine the **pushd** command with command stacking, as in this example: **>> Information# pushd "/cfg/ssl/server 1/ssl" >> SSL Settings#** When you issue the **popd** command, you are immediately return to the prompt where you issued the **pushd** command, the Information prompt in this example.
popd	Return to a position in the menu structure "bookmarked" by using the **pushd** command.
<Ctrl-p>	(Also the up arrow key.) Recall the previous command from the history list. Use this multiple times to work backward through the last 10 commands. The recalled command can be entered as is or edited using the following options.
<Ctrl-n>	(Also the down arrow key.) Recall the next command from the history list. Use this multiple times to work forward through the last 10 commands. The recalled command can be entered as is or edited using the following options.
<Ctrl-a>	Move the cursor to the beginning of command line.
<Ctrl-e>	Move cursor to the end of the command line.
<Ctrl-b>	(Also the left arrow key.) Move the cursor back one position to the left.
<Ctrl-f>	(Also the right arrow key.) Move the cursor forward one position to the right.
<Backspace>	(Also the Delete key.) Erase one character to the left of the cursor position.
<Ctrl-d>	Delete one character at the cursor position.

Option	Description
<Ctrl-k>	Kill (erase) all characters from the cursor position to the end of the command line.
<Ctrl-l>	Rewrites the most recent command.
<Ctrl-c>	Abort an ongoing transaction. If pressed when there is no ongoing transaction, the current menu appears. **Note:** Using Ctrl-c cannot stop screen output generated from using the **cur** command. To stop the heavy screen output that can result from using the **cur** command, press the q key.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

Command Line Interface Shortcuts

Command Stacking

You can type multiple commands separated by forward slashes (/) on a single line to access a submenu and one of the related menu options. Type as many commands as required to access the desired submenu and menu command. For example, the keyboard shortcut to access the **list** command in the NTP Servers menu from the Main menu prompt is as follows.

```
>> Main# cfg/sys/time/ntp/list
```

You can use command stacking to go up one or more levels in the menu system, and then go directly to another submenu and one of the related menu command in that submenu. For example, to go up two levels from the NTP Servers menu to the System menu, and to the DNS settings menu to access the DNS servers menu, you type.

```
>> NTP Servers# ../../dns/servers
```

Command Abbreviation

You can abbreviate most commands by entering the first characters to distinguish the command from the others in the same menu or submenu. You can also enter the command shown in the preceding example as follows:

```
>> Main# c/sy/t/n/l
```

TAB Command Completion

By typing the first letter of a command at any menu prompt and pressing TAB, all commands in that menu that begin with that letter appear. By typing additional letters, you can further refine the list of commands or options displayed. If only one command matches the letters you typed, that command is supplied on the command line when you press TAB. You can then execute the command by pressing ENTER. If you press the TAB key with no input on the command line, the currently active menu appears.

TAB Value Presentation

Press the Tab key to display available options; for example, you can view previously configured values.

```
>> Main# cfg/vpn <id>/linkset <id>/link

 Enter Link number (1-256):  <press TAB>       Windows file
share link(1)            Net
Direct link(2)

Enter Link number (1-256):
```

In the preceding example, with the object name followed by the object ID within parentheses, you can use both the name and the integer (for example 2) to select the object.

Example: To select Net Direct link, enter N, and press Tab. This will complete the object name so that the full name prints. Then press Enter to select this value.

In the following example, with the object ID followed by the object name within parenthesis, you can use only the integer (for example 2) to select the object.

```
>> AAA# defippool <press TAB>

 Usage: defippool <integer> 2(RADIUS)       1(Local)
```

Using Submenu Name as Command Argument

To display the properties related to a specific submenu, you can provide the submenu name as an argument to the **cur** command (at a menu prompt one level up from the desired submenu information).

For example, to display system information at the Configuration menu prompt **(/cfg)**, type the following command.

```
>> Configuration# cur sys

 System:

  Management IP (MIP) address = 192.168.128.211

Cluster Host 1: Type of the host = master
IP address = 192.168.128.213
SysName =
SysLocation =
License =
IPsec user sessions: 250
Secure Service Partitioning
PortalGuard
TPS: unlimited
SSL user sessions: 250
Default gateway address = 192.168.128.3
Ports = 1 : 2
Hardware platform = 3070
Host Routes:
No items configured
Host Interface 1:
IP address = 10.1.82.145
Network mask = 255.255.255.0
Default gateway address = 0.0.0.0
VLAN tag id = 0
Mode = failover
Primary port = 0
Host Interface Routes:
No items configured
```

Without having to descend into the System menu **(/cfg/sys)**, system-specific information appears directly only at the Configuration menu prompt. If the **cur** command was used without the **sys** submenu argument in the preceding example, information related to both the Configuration menu and all submenus appears.

Using Slashes (/) and Spaces in Commands

If you need to use a forward slash (/) or a space in a command string, make sure the string that contains the slash or space is within double quotation marks before you run the command. One example of a command where you use double quotation marks, is when you specify a

directory path and file name on the same line as the **ftp** command in the CLI as shown in the following example.

```
>> Software Management# download ftp 10.0.0.1 "pub/SSL-7.0.1-
upgrade_complete.pkg"
```

IP Address and Network Mask Formats

IP Addresses

You can specify the IP addresses in various ways in the CLI:

- Dotted decimal notation. Specify the IP address as is; for example, **10.0.0.1**.
- According to the formats below: A.B.C.D = A.B.C.D, that is, same as above A.B.D = A.B.0.D, that is, **10.1.10** translates to **10.1.0.10** A.D = A.0.0.D, that is, **10.1**translates to **10.0.0.1** D = 0.0.0.D, that is, **10**translates to **0.0.0.10**

Network Masks

You can enter a network mask in number of bits or in dotted decimal notation.

For example, you can enter the network mask 255.0.0.0 as 8. You can also enter the network mask 255.255.0.0 as 16. You can also enter the network mask 255.255.255.0 as 24. You can also enter the network mask 255.255.255.255 as 32.

Variables

Some of the commands and features in the AVG software use variables. The following table lists available variables and areas and their description.

Variable	Description
<var:user>	Expand to the user name specified when the user logged in to the VPN, for example on the Portal login page. The variable can for example be included in Portal link specifications, in single-sign-on headers (see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244), for proxy mapping (see /cfg/vpn <id> /server/proxymap Proxy Mapping Configuration on page 264), in redirect URLs and static texts (see /cfg/vpn <id> /portal SSL VPN Portal Configuration on page 316).

Variable	Description
<*var:password*>	Expand to the password specified when the user logged in to the VPN. The variable can for example be included in Portal link specifications, in single-sign-on headers (see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244), for proxy mapping (see /cfg/vpn <id> /server/proxymap Proxy Mapping Configuration on page 264) and in redirect URLs (see /cfg/vpn <id> /portal SSL VPN Portal Configuration on page 316).
<*var:group*>	Expand to the group in which the logged on user is a member. The variable can for example be included in Portal link specifications, in single-sign-on headers (see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244), in redirect URLs and static texts (see /cfg/vpn <id> /portal SSL VPN Portal Configuration on page 316).
<*var:portal*>	Expand to the Portal's IP address. The variable can for example be included in single-sign-on headers (see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244) and in redirect URLs (see /cfg/vpn <id> /portal SSL VPN Portal Configuration on page 316).
<*var:domain*>	Expand to the domain name specified for the authentication method by which the logged in user was authenticated. The domain name is specified with the /**cfg /vpn <id>/aaa/auth <id>/domain** command. The variable can, for example, be included in Portal link specifications and in single-sign-on headers (see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244).
<*var:method*>	Expand to the access protocol used, that is, http or https.
<*var:sslsid*>	Expand to the SSL session ID in binary format.
<*var:clicert*>	Expand to a Base 64 encoded version of the client certificate, if one was present when the user was logged in to the VPN. Use this variable to create dynamic HTTP headers (see /cfg/ssl/server <id> /http/dynheader Dynamic Header Configuration on page 108).
<*md5:...*>	Expand the variable or variables (for example <*md5:<user>:<password>*>) and computes an MD5 checksum which is Base 64 encoded. Use this variable to create dynamic HTTP headers (see /cfg/ssl/server <id> /http/dynheader Dynamic Header Configuration on page 108) and single-sign-on headers (see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244).
<*base64:...*>	Expand the variable or variables (for example <*base64:<user>:<password>*>) and encodes them using Base 64. Use this variable to create dynamic HTTP headers (see /cfg/

Variable	Description
	ssl/server <id> /http/dynheader Dynamic Header Configuration on page 108) and single-sign-on headers (see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244).
<*var:tgFailureReason*>	Expand to the Tunnel Guard rule expression and the Tunnel Guard rule comment specified for the current SRS rule when a Tunnel Guard check failed. For more information, see the "Configure Tunnel Guard" chapter in the *Application Guide for VPN*.
<*var:tgFailureDetail*>	Expand to the software definition comment specified for the current SRS rule, along with a detailed specification of missing, present files, processes generated by the Tunnel Guard applet when a Tunnel Guard check failed. For more information, see the "Configure Tunnel Guard" chapter in the*Application Guide for VPN*. **Note:** This variable is not expanded if **`/cfg/vpn <id>/aaa/tg/details`** is set to **off** .
Operator-defined variables	Create custom variables to retrieve the desired values from RADIUS and LDAP databases (see /cfg/vpn <id> /aaa/auth <id> /radius/macro RADIUS Macro Configuration on page 175 and /cfg/vpn <id> /aaa/auth <id> /ldap/ldapmacro LDAP Macro Configuration on page 186).

Note:

Variables included in links are URL encoded whereas variables included in static texts (for example, on the Portal page and on the Portal login page) are not URL encoded.

The Main Menu

The Main menu appears after a successful connection and login. Main menu appears if you logon as an Administrator. Note that some of the commands are not available who logged in as Operator.

```
[Main Menu]
      info       - Information menu
      stats      - Statistics menu
      cfg        - Configuration menu
      boot       - Boot menu
      maint      - Maintenance menu
      diff       - Show pending config changes   [global command]
      apply      - Apply pending config changes  [global command]
      revert     - Revert pending config changes [global command]
      paste      - Restore saved config with key [global command]
      help       - Show command help             [global command]
      exit       - Exit  [global command, always available]
```

Menu Summary

- Information menu

  Provides submenus for to display information about the current status of the VPN Gateway. For more information, see /info Information Menu on page 31.

- Statistics menu

  Provides submenus for to display AVG performance statistics. For more information, see /stats Statistics Menu on page 48.

- Configuration menu

  Provides submenus to configure the AVG cluster, for example for SSL offload and VPN deployment. Some of the commands in the Configuration menu are available only who logged in as the Administrator user. For more information, see /cfg Configuration Menu on page 81.

- Boot menu

  Is used to upgrade AVG software and to reboot, if necessary. The Boot menu is accessible only who logged in as the Administrator user. For more information, see /boot Boot Menu on page 454.

- Maintenance menu

  Is used to send technical support information to an FTP/TFTP/SFTP server. For more information, see /maint Maintenance Menu on page 457.

/info Information Menu

The Information menu is used to view information and events for VPN Gateways in a cluster.

```
[Information Menu]
      servers    - Show configured SSL servers
      certs      - Show configured certificates
      hsm        - Show local HSM information
      sslvpn     - Show configured VPNs
      users      - Show logged in SSL VPN portal users
      idleusers  - Show idle logged in SSL VPN portal users
      ipsec      - Show logged in IPSEC users
      botuns     - Show IPsec BO tunnels
      ippool     - Show ip pool allocations
      hippool    - Show host ip pool allocations
      ip         - Find information about an IP address
      sys        - Show system configuration
      licenses   - Show SSL VPN portal license usage
      access     - Print the access rules of an SSL VPN portal user
      kick       - Kick an SSL VPN portal user
      isdlist    - Show all hosts and their operational status
      local      - Show local host information
      ethernet   - Show local ethernet status information
      ports      - Show local port(s) information
      id         - Show user name and groups for current user
      events     - Inspect Events menu
      sonmp      - SONMP topology
```

The following table shows the various Information menu options.

Table 3: Information Menu Options (/info)

Command Syntax and Usage
servers Display the current SSL server settings, including SSL specific settings for each configured virtual SSL server.
certs Display the certificate name, serial number, expiration date, and key size for each installed certificate. Information related to the subject part of the certificate is also displayed.
hsm Display status information related to the HSM cards on each AVG device in the cluster. Information about the current security mode (Extended mode or FIPS mode) is displayed, as well as current login status and login user information (HSM-SO or HSM-USER). For a sample screen output, see /info/hsm HSM Command on page 38. **Note:** HSM information is only displayed when you are using the ASA 310-FIPS model.
sslvpn Display information about the current SSL VPN settings, for example login session idle timeout value (shared by all configured VPNs), as well as information related to each specific VPN configuration. For each VPN, information about authentication methods, authentication order, user access groups and the access rules associated with each group is displayed.

Command Syntax and Usage	
users <*VPN ID*> <*prefix*>	
Display the user name, login time, source IP address, access method (SSL or IPsec), group membership and profile of all remote users that are currently logged in to a VPN. The users are listed per VPN.	
Examples of argument use:	
>> Information# **users**	Lists all currently logged in users for all VPNs.
>> Information# **users 2**	Lists all users currently logged in to VPN 2.
>> Information# **users 2 j***	Lists users currently logged in to VPN 2, whose user name begins with the letter " j ".
>> Information# **users 2 joe**	Lists users currently logged in to VPN 2, whose user name is exactly " joe ".
For sample output, see /info/users Users Command on page 39.	
idleusers <*number of seconds*> <*VPN ID*> <*prefix*>	
List all users that have been idle longer than the time specified in the command argument.	
Examples of argument use:	
>> Information# **idle 30**	Lists all SSL users who have been idle more than 30 seconds.
>> Information# **idle 5m 2**	Lists all SSL users currently logged in to VPN 2 who have been idle more than 5 minutes.
>> Information# **idle 1h 2 j***	Lists all SSL users currently logged in to VPN 2, whose user name begins with the letter " j ", who have been idle more than 1 hour.
>> Information# **idle 1h 2 joe**	Lists all SSL users currently logged in to VPN 2, whose user name is exactly " joe ", who have been idle more than 1 hour.
The information includes VPN ID, user name, login time, last time active, source IP address and access method. For sample output, see /info/idleusers Idleusers Command on page 39.	
ipsec <*VPN ID*> <*prefix*>	

Command Syntax and Usage	
Show currently logged in IPsec users. The information includes user name, user tunnel profile name, actual source IP address, new source IP address allocated from IP pool, encrypted/decrypted data in kBytes and session length.	
Examples of argument usage:	
`>> Information# ipsec`	Lists all currently logged in users for all VPNs.
`>> Information# ipsec 2`	Lists all users currently logged in to VPN 2.
`>> Information# ipsec 2 s*`	Lists all users currently logged in to VPN 2, whose user tunnel profile name begins with the letter " s ".
`>> Information# ipsec 2 staff`	Lists users currently logged in to VPN 2, whose user tunnel profile name is exactly " staff ".
For a sample screen output, see /info/ipsec Ipsec Command on page 40.	
Note: This command is not available if the VPN Gateway software runs on the ASA 310 or ASA 410 hardware platforms.	
botuns <*VPN ID*> <*prefix*>	
Show the number of active branch office tunnel sessions for all VPNs. The information includes branch office tunnel profile name, the AVG host from which the tunnel is set up, the tunnel state, encrypted/decrypted data in kBytes and session length.	
Examples of argument usage:	
`>> Information# botuns`	Lists all currently active branch office tunnels for all VPNs.
`>> Information# botuns 2`	Lists all currently active branch office tunnels for VPN 2.
`>> Information# botuns 2 d*`	Lists all currently active branch office tunnels for VPN 2, whose tunnel profile name begins with the letter " d ".
`>> Information# botuns 2 denver`	Lists all currently active branch office tunnels for VPN 2, whose tunnel profile name is exactly " denver ".
For sample output, see /info/botuns Botuns Command on page 40.	
ippool <*VPN ID*>	

Command Syntax and Usage	
Show IP pool allocations per IP pool and VPN. The information includes configured IP address range, free IP addresses or ranges and currently allocated IP addresses. It also shows which VPN Gateway (iSD) that owns the IP address.	
Examples of argument use:	
`>> Information# ippool`	Shows IP pool allocations for all VPNs.
`>> Information# ippool 2`	Shows IP pool allocations for VPN 2.
For sample output, see /info/ippool Ippool Command on page 41.	
hippool <*vpn id*>	
Shows the host IP pool allocations for each IP pool and VPN. The information includes configured IP address range, free IP addresses or ranges and currently allocated IP addresses. It also shows which VPN Gateway (iSD) that owns the IP address.	
Examples of argument use:	
`>> Information# hippool`	Shows host IP pool allocations for all VPNs.
`>> Information# hippool 2`	Shows host IP pool allocations for VPN 2.
For sample output, see /info/hippool hippool Command on page 43.	
ip <*IP address*>	
Find information about a specific IP address allocated from the IP address pool. The information includes the VPN Gateway that owns the IP address, to which VPN the remote user has connected, user name, actual source IP, login time, user groups to which the user belongs, source IP allocated from IP pool and user profile information (access method, source IP, authentication server, client certificate present, IE cache wiper running, Tunnel Guard activated, domain). For sample output, see /info/ip Ip Command on page 44.	
sys	
Display information about the current system configuration, for example network mask, default gateway address, static routes, NTP servers, DNS servers, syslog servers, networks, number of VPN Gateways included in the cluster along with IP addresses and so on.	
licenses <*VPN ID*>	
Show information about the license pool and current usage per VPN and license type. To limit the presentation to a specific VPN, enter the desired VPN ID following the command. Example:	

Command Syntax and Usage
`>> Information# licenses 2` For a sample screen output, see /info/licenses Licenses Command on page 45.
access <*VPN ID*> <*user name*>
By specifying a VPN number and a user name following the **access** command, a detailed view of a logged in user's access rights is displayed. The information is presented in a table showing the user's access rights to specific networks, ports, protocols and paths.
kick <*VPN ID*> <*user name*>
By specifying the desired VPN number and a user name following the **kick** command, a user or all matched users can be logged out from a VPN session by the operator. To log out multiple users, for example selected users or a range of users, enter an asterisk when prompted for user name. Currently logged in users are displayed in list format with an index number. Enter the index numbers corresponding to the users you wish to log out. Example: To log out users corresponding to index numbers 1-3 and 5, enter **1-3, 5**.
isdlist
Display the IP addresses, master/slave assignments, CPU usage, memory usage, operational status, and uptime for all the VPN Gateways in the cluster. An asterisk (*) in the MIP column indicates which VPN Gateway in the cluster is currently is control of the Management IP. An asterisk (*) in the Local column indicates the particular VPN Gateway to which you have connected. For a sample screen output, see /info/isdlist iSD List Command on page 46.
local
Display the current software version, hardware platform, up time (since last boot), IP address, and Ethernet MAC address for the particular VPN Gateway to which you have connected. If you have connected to the MIP address, the information displayed relates to the VPN Gateway in the cluster that currently is in control of the MIP. For a sample screen output, see /info/local Information Local Command on page 46.
ethernet
Display statistics for the Ethernet network interface card (NIC) on the particular VPN Gateway to which you have connected. If you have connected to the MIP address, the information displayed relates to the VPN Gateway in the cluster that currently is in control of the MIP. If more than one network is configured in the cluster, ethernet statistics for the respective network is displayed. • `RX packets` : the total number of received packets • `TX packets:` the total number of transmitted packets

Command Syntax and Usage
• `errors:` packets lost due to error • `dropped:` error due to lack of resources • `overruns:` error due to lack of resources • `frame:` error due to malformed packets • `carrier:` error due to lack of carrier • `collisions:` number of packet collisions • `RX bytes:` received packets in bytes • `TX packets:` transmitted packets in bytes For a sample screen output, see /info/ethernet Information Ethernet Command on page 47. **Note:** A non-zero collision value may indicate an incorrect configuration of the Ethernet autonegotiation. For more information, see the **autoneg** command on autoneg on|off.
ports
Displays the status of the physical ports on the Ethernet network interface card (NIC) on the particular VPN Gateway to which you have connected. If you have connected to the MIP address, the information displayed relates to the VPN Gateway in the cluster that currently is in control of the MIP. For each port, link status (up/down) and the Ethernet autonegotiation setting (on/off) is shown. If the link is up, current values for speed (10/100/1000) and duplex mode (half/full) are also shown. If the link is down and autonegotiation is set to off, the configured values for speed and duplex mode are shown instead. To change the NIC port settings, see the commands under .
id
Shows user name and groups for the currently logged in administrator user. The primary purpose of the command is to verify the group assignment when using RADIUS authorization of CLI/BBI users (see the **/cfg/sys/adm/auth/group** command on /cfg/sys/adm/auth/group RADIUS Group Attribute Configuration on page 440).
events
Displays the Events menu. To view menu options, see /info/events Events Menu on page 38.
sonmp
Display information about the current network topology, if SONMP participation is enabled (using the **/cfg/sys/adm/sonmp** command). For sample output, see /info/sonmp Sonmp Command on page 47.

/info/events Events Menu

```
[Events Menu]
alarms     - List all pending alarms
download   - Dump the event log file to a TFTP/FTP/SFTP server
```

The Events menu is used for viewing active alarms and events that have been logged.

Table 4: Events Menu Options (/info/events)

Command Syntax and Usage
alarms Displays all alarms in the active alarm list by their main attributes: severity level, alarm ID number, date and time when triggered, alarm name, sender, and cause. To alert the operator at system login, a notice is displayed if there are active alarms. Alarms are also sent as syslog messages.
download *<method (TFTP/FTP/SFTP)> <host name or IP address> <file name on host>* Transmits the event log file from the AVG cluster to a file on a TFTP/FTP/SFTP server. You need to specify the IP address or host name of the server, as well as a file name. The default value is **tftp**.

/info/hsm HSM Command

```
>> Information# hsm

 iSD IP 192.168.128.185:

  Mode: Extended

  HSM card 0: Logged in as HSM-USER HSM card 1: Logged in as
HSM-USER

  HSM card 1: Logged in as HSM-USER
```

The output shows status information related to the HSM cards on each AVG device in the cluster. Information about the current security mode (Extended mode or FIPS mode) is displayed, as well as current login status and login user information (HSM-SO or HSM-USER).

/info/users Users Command

```
>>Main # /info/users

Number of currently logged in users:1

VPN ID     User   Login   SourceIP     Acces   Group:Profile:U
                                       s       sers

1          john   05:46   47.102.177   ssl     trusted:avaya
                          .57                  trusted:<base>
                          134.177.220          domain="vmdomai
                          .29                  n"
```

The output shows VPN ID, name of logged in Portal user, login time, source IP per access method (SSL, IPsec, Net Direct, or SPO), host IP (of the AVG to which the user is connected), access method (SSL, IPsec, Net Direct or SPO), group membership, profile, and current owner of the session (User currently logged into the AVG cluster). The <base> profile refers to data configured directly under the Group menu. Any other profile stated after the group name is an extended profile. For more information about base profiles and extended profiles, see the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN*.

If values are retrieved from LDAP or RADIUS authentication servers through variables, the variable name and the retrieved value is also displayed. For more information about LDAP and RADIUS variables, see /cfg/vpn <id> /aaa/auth <id> /ldap/ldapmacro LDAP Macro Configuration on page 186 and /cfg/vpn <id> /aaa/auth <id> /radius/macro RADIUS Macro Configuration on page 175 respectively.

If Tunnel Guard is enabled, if the user failed the Tunnel Guard check and if the variables *<var:tgFailureReason>* and/or *<var:tgFailureDetail>* have values configured, these values are printed as a result of the Tunnel Guard check. Note that the *<var:tgFailureDetail>* variable is not expanded if the **`/cfg/vpn <id>/aaa/tg/details`** command is set to **`off`**. You can read more about these variables in the section Variables on page 28.

/info/idleusers Idleusers Command

```
>> Information# idleusers

  Number of users idle more than 30s: 2

  VPN Id User              Login   Active       Source
IP  Access...
```

```
   ------ ----               -----    ------
  ---------  ---------

  1 lisa              13:13    13:15   192.168.128.19     ssl
2 john               13:28    13:39   192.168.128.31     ssl
```

The output shows VPN ID, user name, login time, last time active, source IP address and access method.

/info/ipsec Ipsec Command

```
>> Information# ipsec

Number of active ipsec user sessions for all VPNs: 1

------ VPN Number: '1' ------

User:      TunProf    IP Inner/  Enc (Kb)   Dec (kB)   Time
                      Outer

john       vpn_1_1    10.1.82.1  0          0          0:01:55
                      48/192.16
                      8.128.19
```

The output shows the user name of the IPsec user and the user tunnel profile, the inner IP address (that is, the IP address allocated from the IP pool/RADIUS for the unencrypted connection between the VPN Gateway and the destination host), the outer IP address (that is, the IP address from which the remote user connects to the VPN Gateway), encrypted data in kBytes and decrypted data in kBytes. The output also shows the time the tunnel has been active (hours:minutes:seconds).

/info/botuns Botuns Command

```
>> Information# botuns

Number of enabled BO tunnels for all VPNs: 3

------ VPN Number: '1' ------

Number of enabled BO tunnels: 1

Number of   down:1    phase1:0  up:0
BO tunnels
in state:
```

```
BotunProf   At host   State     Enc (KB)  Dec (KB)  Time
denver(1)   1         down      0         0         07:04:36
----- VPN Number: '2' -----
Number of enabled BO tunnels: 2
Number of   down:0    phase1:0  up:1
BO tunnels
in state:
BotunProf   At host   State     Enc (KB)  Dec (KB)  Time
austin(2)   1         down      0         0         00:00:05
dallas(1)   2         up        143       138       09:01:25
------ VPN Number: ’3’ ------
Number of enabled BO tunnels: 0
Number of   down:0    phase1:0  up:0
BO tunnels
in state
BotunProf   At host   State     Enc (KB)  Dec (KB)  Time
------ VPN Number: ’4’ ------
Number of enabled BO tunnels: 0
Number of   down:0    phase1:0  up:0
BO tunnels
in state
```

The output shows the name of the branch office tunnel profile, the AVG host from which the tunnel is set up, the tunnel state (`up, phase1` or `down`), encrypted data in kBytes and decrypted data in kBytes. The `up` tunnel state means that both ISAKMP and IPsec SAs are established, whereas the `phase1` state indicates that only the ISAKMP SA is established).

The output also shows the time the tunnel has been active (hours:minutes:seconds).

/info/ippool Ippool Command

```
>> information ippool

*** Pool '1' for 'VPN 2'
```

```
type = local

proxyarp= on

hostroute= false

range= 2.2.2.2.-2.2.2.100

free=
                                2.2.2.2

                                2.2.2.3

                                2.2.2.4

                                2.2.2.5

                                2.2.2.6

                                2.2.2.7

                                2.2.2.8

                                2.2.2.9

                                2.2.2.10

                                2.2.2.11

                                2.2.2.12

                                2.2.2.13

                                2.2.2.14

                                2.2.2.15

                                2.2.2.16
```

```
franges=
                                    10.1.82.102-10.1.82.149
alloc = (2 allocated IP addresses)
'isd@a10-1-82-200' has 10.1.82.100
'isd@a10-1-82-205' has 10.1.82.101
```

The output shows IP pool information per IP pool and VPN. The information includes configured IP address range, free IP addresses or ranges and currently allocated IP addresses. It also shows which VPN Gateway (iSD) that owns the IP address.

An IP address from the IP pool is allocated as source IP address to unencrypted connections between the VPN Gateway and the requested destination when the remote user connects to the VPN Gateway through the Net Direct client or the Avaya VPN client (formerly the Contivity VPN client).

/info/hippool hippool Command

Following is the output for /info/hippool with two host members in a cluster:

```
>> Main# /info/hippool

  *** Pool '2' for VPN '1'
type:      local
proxyarp:  on
hostroute: false
** Host 134.177.220.65
range     = 11.11.11.1-11.11.11.3
free      =
11.11.11.1
11.11.11.2
11.11.11.3
franges   =
alloc     = (0 allocated IPs)
*** Pool '2' for VPN '1'
type:      local
proxyarp:  on
hostroute: false

  ** Host 134.177.220.249
range     = 10.20.30.1-10.20.30.4
free      =
10.20.30.2
```

```
10.20.30.3
10.20.30.4
franges    =
alloc      = (1 allocated IPs)
'isd@a134-177-220-249'  has 10.20.30.1
```

The output shows host IP pool information for each IP pool and VPN. The information includes configured host IP address, IP address range, free IP addresses or ranges and currently allocated IP addresses. It also shows which VPN Gateway (iSD) that owns the IP address.

/info/ip Ip Command

Following is the output for /info/ip when the IP is allocated from a host IP Pool when the hostippool feature is enabled:

```
>> Information# ip

Enter IP to search for: 10.20.30.1
IP 10.20.30.1 not allocated from IP
pool
IP 10.20.30.1 allocated at
'isd@a134-177-220-249' by netdirect
at node 'isd@a134-177-220-249'
(VPNid='1' POOLid='2'
Host=134.177.220.249)
--- Node 'isd@a134-177-220-249' ---

VPN:         '1'
User:        test
Src IP:      134.177.220.97
Login:       16:56
Groups:      trusted

Src:

ssl     134.177.220.97  Groups:
trusted
netdir  10.20.30.1      Groups:
trusted

Prof:

Access:      ssl
SrcIp:       134.177.220.97
AuthSrv:     local
ClientCert:  false
IE Wiper:    false
TunnelGuard: false
```

```
Nap:        undefined
Domain:
```

The output shows information about the VPN Gateway that owns the IP address, to which VPN the remote user has connected, user name, actual source IP, login time, user groups to which the user belongs, source IP allocated from IP pool and user profile information (access method, source IP, authentication server, client certificate present, IE cache wiper running, Tunnel Guard activated, domain).

/info/licenses Licenses Command

```
>> Information# licenses
Global License  VPN             Used            Size
Pools
-------------------------------------------------------------------------------------------------------------
------------------
SSL             -               0               50
SSL             1               1               20
SSL             2               3               30
IPSEC           -               0               20
Vdesk           1               3               25
SPIKE           2               1               10
License usage   VPN             Used
per
-------------------------------------------------------------------------------------------------------------
---------------------
SSL             1               0
SSL             2               3
SSL             3               0
IPSEC           1               0
IPSEC           2               2
IPSEC           3               0
Vdesk           1               0
Vdesk           2               0
```

```
Vdesk           3               0
Vdesk           4               3
SPIKE           1               1
SPIKE           2               0
```

The output shows 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 (that is, SSL and IPsec) and if the Secure Service Partitioning feature is used for each VPN.

In the preceding example, a 100 user SSL license is loaded to the cluster. The top table's `Size` column shows how the administrator has set a limit of 20 concurrent users for VPN no 1 and 30 to VPN no 2. The remaining 50 are not allocated and thus available to other VPNs in the cluster. Only the VPNs with a configured license allocation are included in this table.

The bottom table which includes all VPNs shows license usage per VPN and license type. The preceding example reveals that a third VPN exists in the cluster and that 22 remote users belonging to that VPN are currently logged in.

/info/isdlist iSD List Command

```
>> Information# isdlist
IP addr         type   MIP Local cpu(%) mem(%)  op    Uptime
10.127.232.51   master  *    *     1     16     up    6 days 17 hour
10.127.232.52   master  *    *     1     16     up    6 days 17 hour
10.127.232.53   master  *    *     1     16     up    6 days 17 hour
```

The output shows the IP addresses, master/slave assignments, CPU usage, memory usage, operational status, and uptime for all the VPN Gateways in the cluster. An asterisk (*) in the MIP column indicates which VPN Gateway in the cluster is currently is control of the Management IP. An asterisk (*) in the Local column indicates the particular VPN Gateway to which you have connected.

/info/local Information Local Command

```
>> Information# local

 Alteon iSD SSL
Hardware platform: 3070
Software version 7.0.1
Up time: 5 days 21 hours 40 minutes
```

```
IP address: 192.168.128.185
MAC address: 00:01:02:b1:25:c0
```

The output shows the current software version, hardware platform, up time (since last boot), IP address, and Ethernet MAC address for the particular VPN Gateway to which you have connected. If you have connected to the MIP address, the information displayed relates to the VPN Gateway in the cluster that currently is in control of the MIP.

/info/ethernet Information Ethernet Command

```
>> Information# ethernet

 Net 1: RX packets:2618 errors:0 dropped:0 overruns:1 frame:
0
Net 1: TX packets:221 errors:0 dropped:0 overruns:0 carrier:
0 collisions:0
Net 1: RX bytes:192038 (187.5 Kb)   TX bytes:13298 (12.9 Kb)
```

The output shows statistics for the Ethernet network interface card (NIC) on the particular VPN Gateway to which you have connected. If you have connected to the MIP address, the information displayed relates to the VPN Gateway in the cluster that currently is in control of the MIP. If more than one network is configured in the cluster, ethernet statistics for the respective network is displayed.

/info/sonmp Sonmp Command

```
>> Information# sonmp

Slot IP address   Seg MAC address        Chassis Type Local
State Port                  Id                          Seg
---- ----------- --- ---------------- ------------ -----
-----
0/0   10.1.82.145   0   00:07:e9:13:a6:dd
NnVPNGw3070 true heartbeat
1/1   10.1.0.10     303 00:09:97:f3:b4:aa
ERS5510-48T   true   heartbeat
1/1   10.1.82.2     275 00:80:2d:7e:ab:ea
BayStack450   true   new
```

The table lists all SONMP-aware Network Management Modules (NMMs) on the same network as the reporting NMM (the VPN Gateway). A table entry is created when a topology message

is sent from a "new" NMM. An entry is removed when no topology messages are received from the NMM within a specified time interval.

`Slot`	The slot (on the port) on which the topology message was received. The reporting agent's row has slot number equal to zero (see top row in the preceding example).
`Port`	The port on which the topology message was received. The reporting agent's row has port number equal to zero (see top row in the preceding example).
`IP address`	IP address of the interface on which the topology message was received. Seg Id Identifies the network segment in the NMM from which the topology message was sent.
`MAC address`	The MAC address of the NMM sending the topology message.
`Chassis Type`	The chassis type (product name) of the NMM sending the topology message.
`Local Seg`	Indicates whether or not the NMM is located on the same network segment (local) as the reporting NMM or across a bridge.
`State`	Indicates the state of the NMM. Available values are `topChanged` (topology value has recently changed), `heartbeat` (topology information unchanged and `new` (sending agent is in new state).

Note:

Only the NMM topology table is tracked, not the bridge topology table.

/stats Statistics Menu

The Statistics menu is used for accessing performance statistics for the VPN Gateway software's main features.

```
[Statistics Menu]
      sslstats    - SSL stats
      ipsec       - IPSEC stats
      aaa         - AAA specific statistics
      dump        - Dump all information
```

Table 5: Statistics Menu Options (/stats)

Command Syntax and Usage
sslstats Displays the SSL statistics menu. To view menu options, see /stats/sslstats SSL Statistics Menu on page 49.

Command Syntax and Usage
ipsec
Displays the IPsec statistics menu. To view menu options, see /stats/ipsec IPsec Statistics Menu on page 67.
Note: This command is not available if the VPN Gateway software is run on the ASA 310 or ASA 410 hardware platforms.
aaa
Displays the AAA statistics menu. To view menu options, see /stats/aaa AAA Statistics Menu on page 78.
dump
Displays cluster-wide SSL statistics for each virtual SSL server in the cluster, as well as the number of active request sessions, and the total number of completed request sessions. The total number of initiated SSL client connections, and the total number of established SSL client connections as accumulated values for all virtual SSL servers in the cluster are also displayed. Histograms, however, are not included in the output.

/stats/sslstats SSL Statistics Menu

```
[SSL stats Menu]
      vpn        - Cluster SSL VPN statistics
      server     - Cluster SSL Server statistics
      local      - Local statistics for each isdhost
      clear      - Clear all statistics for all IPs
      activesess - Number of currently active request sessions
      totalsess  - Total completed request sessions
      sslaccept  - Total completed SSL accept
      sslconnect - Total completed SSL connect
      tpshisto   - Cluster-wide TPS histograms for all servers
      clihisto   - cluster wide client data histograms for all servers
      srvhisto   - cluster wide server data histograms for all servers
```

The SSL Statistics menu is used for viewing various statistics relating to SSL sessions.

Table 6: SSL Statistics Menu Options (/stats/sslstats)

Command Syntax and Usage
vpn
Displays the Cluster Wide SSL Statistics menu for the specified VPN (that is, the portal server of that domain). To view menu options, see /stats/sslstats/vpn <number> Cluster Wide SSL Statistics for VPN Menu on page 53.
server *<virtual SSL server number>*

Command Syntax and Usage
Displays the Cluster Wide SSL Statistics menu for the specified virtual SSL server (that is, servers configured under **/cfg/ssl**). Press TAB following this command to view the numbers of configured servers. To view menu options, see /stats/sslstats/server <number> Cluster Wide SSL Statistics for Server Menu on page 55.
local
Displays the Local Statistics menu. To view menu options, see /stats/sslstats/local Local SSL Statistics Menu on page 58.
clear
Resets all statistics to zero.
activesess
Displays the number of currently active request sessions in the cluster.
totalsess
Displays the total number of completed request sessions in the cluster.
sslaccept
Displays the total number of initiated SSL client connections on all virtual SSL servers in the cluster.
sslconnect
Displays the total number of established SSL client connections on all virtual SSL servers in the cluster.
tpshisto
Displays histograms of the number of SSL transactions per second, as performed by each virtual SSL server in the cluster. The figures presented are accumulated from all AVG devices in the cluster. For a sample screen output, see /stats/sslstats/tpshisto Cluster-Wide TPS Histogram for All Servers on page 51.
clihisto
Displays histograms of data throughput in bytes per second from clients to each virtual SSL server in the cluster. The figures presented are accumulated from all AVG devices in the cluster. For a sample screen output, see /stats/sslstats/clihisto Cluster-Wide Client Data Throughput Histogram for All Servers on page 51.
srvhisto
Displays histograms of data throughput in bytes per second from backend servers to each virtual SSL server in the cluster. The figures presented are accumulated from all AVG devices in the cluster. For a sample screen output, see /stats/sslstats/srvhisto Cluster-Wide Server Data Throughput Histogram for All Servers on page 52.

/stats/sslstats/tpshisto Cluster-Wide TPS Histogram for All Servers

```
Cluster wide histograms for all Servers
10.1.82.146:443       Histogram SSL tps (last 60 secs)
sec(0)    0     0     0     0     0     0     0     0
sec(8)    0     0     0     0     0     0     0     0
sec(16)   0     0     0     0     0     0     0     0
sec(24)   0     0     0     0     0     0     0     0
sec(32)   0     0     0     0     0     0     0     0
sec(40)   0     0     0     0     0     0     0     0
sec(48)   0     0     0     0     0     0     0     0
sec(56)   0     0     0     0
10.1.82.146:443 Histogram medium tps (last 60 mins)
min(0)    0     0     0     0     0     0     0     0
min(8)    0     0     0     0     0     0     0     0
min(16)   0     0     0     0     0     0     0     0
min(24)   0     0     0     0     0     0     0     0
min(32)   0     0     0     0     0     0     0     0
min(40)   0     0     0     0     0     0     0     0
min(48)   0     0     0     0     0     0     0     0
min(56)   0     0     0     0
10.1.82.146:443 Histogram medium tps (last 24 hours)
hour(0)   0     0     0     0     0     0     0     0
hour(8)   0     0     0     0     0     0     0     0
hour(16)  0     0     0     0     0     0     0     0
10.1.82.146:443 Histogram medium tps (last 31 days)
day(0)    0     0     0     0     0     0     0     0
day(8)    0     0     0     0     0     0     0     0
day(16)   0     0     0     0     0     0     0     0
day(24)   0     0     0     0     0     0     0
```

The output shows the number of SSL transactions per second, as performed by each virtual SSL server in the cluster of VPN Gateways. It is divided in the following sections per virtual SSL server:

- SSL transactions per each of the last 60 seconds.
- Average number of transactions per second during the last 60 minutes.
- Average number of transactions per second during the last 24 hours.
- Average number of transactions per second during the last 31 days.

/stats/sslstats/clihisto Cluster-Wide Client Data Throughput Histogram for All Servers

```
Cluster wide histograms for all Servers
10.1.82.146:443       Histogram client data byte/s (last 60 secs)
```

```
sec(0)     0      0      0      0      0      0      0      0
sec(8)     0      0      0      0      0      0      0      0
sec(16)    0      0      0      0      0      0      0      0
sec(24)    0      0      0      0      0      0      0      0
sec(32)    0      0      0      0      0      0      0      0
sec(40)    0      0      0      0      0      0      0      501
sec(48)    0      0      0      0      0      0      0      0
sec(56)    0      0      0      0
10.1.82.146:443 Histogram medium client data byte/s (last 60 mins)
min(0)     8      2131   1052   0      0      0      0      0
min(8)     0      0      0      0      0      0      0      0
min(16)    0      0      0      0      0      0      0      0
min(24)    0      0      0      0      0      0      0      0
min(32)    0      0      0      0      0      0      0      0
min(40)    0      0      0      0      0      0      0      0
min(48)    0      0      21     0      0      0      0      0
min(56)    0      0      0      0
10.1.82.146:443 Histogram medium client data byte/s (last 24 hours)
hour(0)    0      0      0      0      0      0      0      0
hour(8)    0      0      0      0      0      0      0      0
hour(16)   0      0      0      0      0      0      0      0
10.1.82.146:443 Histogram medium client data byte/s (last 31 days)
day(0)     0      0      2      0      0      0      0      0
day(8)     0      0      0      0      0      0      0      0
day(16)    0      0      0      0      0      0      0      0
day(24)    0      0      0      0      0      0      0
```

The output shows the data throughput in bytes per second from clients to each virtual SSL server in the cluster. It is divided in the following sections per virtual SSL server:

- Data throughput per each of the last 60 seconds.
- Average data throughput per second during the last 60 minutes.
- Average data throughput per second during the last 24 hours.
- Average data throughput per second during the last 31 days.

/stats/sslstats/srvhisto Cluster-Wide Server Data Throughput Histogram for All Servers

```
Cluster wide histograms for all Servers
10.1.82.146:443       Histogram server data byte/s (last 60 secs)
sec(0)     0      0      0      0      0      0      0      0
sec(8)     0      0      0      0      0      0      0      0
sec(16)    0      0      0      0      0      0      0      0
sec(24)    0      0      0      0      0      0      335    0
sec(32)    0      0      0      0      0      0      0      0
sec(40)    0      0      0      0      0      0      0      0
sec(48)    0      0      0      0      0      0      0      0
sec(56)    0      0      0      0
10.1.82.146:443 Histogram medium server data byte/s (last 60 mins)
min(0)     5      5      5      5      5      5      5      4006
min(8)     7349   0      0      0      0      0      0      0
```

```
min(16)    0      0      0      0      0      0      0      0
min(24)    0      0      0      0      0      0      0      0
min(32)    0      0      0      0      0      0      0      0
min(40)    0      0      0      0      0      0      0      0
min(48)    0      0      0      0      0      0      0      0
min(56)    321    0      0      0
10.1.82.146:443 Histogram medium server data byte/s (last 24 hours)
hour(0)    5      0      0      0      0      0      0      0
hour(8)    0      0      0      0      0      0      0      0
hour(16)   0      0      0      0      0      0      0      0
10.1.82.146:443 Histogram medium server data byte/s (last 31 days)
day(0)     0      0      21     0      0      0      0      0
day(8)     0      0      0      0      0      0      0      0
day(16)    0      0      0      0      0      0      0      0
day(24)    0      0      0      0      0      0      0
```

The output shows the data throughput in bytes per second from backend servers to each virtual SSL server in the cluster. It is divided in the following sections per virtual SSL server:

- Data throughput per each of the last 60 seconds.
- Average data throughput per second during the last 60 minutes.
- Average data throughput per second during the last 24 hours.
- Average data throughput per second during the last 31 days.

/stats/sslstats/vpn <number> Cluster Wide SSL Statistics for VPN Menu

```
[Cluster wide SSL Stats for VPN 1 Menu]
      accept     - SSL accept
      handshakeg - SSL handshakes completed
      cachemisse - SSL cache misses
      cachetimeo - SSL cache timeout
      cachefull  - SSL cache full
      cachehits  - SSL cache hits
      sslconnect - SSL connects
      revocation - Client cert revocations
      cipherrewr - HTTP weak cipher rewrites
      http_redir - HTTP redirect rewrites
      becnctfail - Failed backend server connects
      tps        - SSL transactions/sec
      tpshisto   - cluster wide TPS histograms for this server
      clihisto   - cluster wide client byte/s  histos for this server
      srvhisto   - cluster wide server data byte/s histos for this server
      dump       - Print all stats except histograms
```

The Cluster Wide SSL Statistics for VPN menu is used for viewing various statistics for a specific VPN, specified by its ID. The figures presented are accumulated from all AVG devices in the cluster, but specific for the selected VPN.

Table 7: Cluster Wide SSL Statistics for VPN Menu Options (/stats/sslstats/vpn)

Command Syntax and Usage
accept Display the number of initiated SSL client connections for the current virtual VPN.
handshakeg Display the number of successfully completed SSL handshakes for the current VPN. The number of failed SSL handshakes equals the **SSL accept** , minus the combined values for **SSL handshakes completed** and **Number of currently active request sessions**. You can view the values mentioned above by using the **/stats/dump** command.
cachemisse Display the number of times clients have made requests to reuse a particular session ID, and that session ID was not found in the SSL cache. If there is a high number of cache misses in combination with a high value for **cachefull**, you may consider increasing the SSL cache size of the virtual SSL server. To change the current SSL cache size, use the **/cfg/vpn <id>/server/ssl/cachesize** command. The default SSL cache size is 4000 items. If there is a high number of cache misses in combination with a low value for **cachefull**, you may consider increasing the **cachettl** value. To change the current cachettl value, use the **/cfg/vpn <id>/server/ssl/cachettl** command. The default SSL cache timeout value is 5 minutes.
cachetimeo Displays the number of reuse attempts on SSL sessions still in the cache, and whose timeouts were initiated. If there is a high number of cache timeouts, you may consider increasing the **cachettl** value for the virtual SSL server using the **/cfg/vpn <id>/server/ssl/cachettl** command. The default SSL cache timeout value is 5 minutes.
cachefull Displays the number of times when a new client session could not be cached due to the cache being full. If the **cachefull** value is high, you may consider increasing the SSL cache size of the virtual SSL server.
cachehits Displays the number of times clients have made requests to reuse a particular session ID, and that session ID was found in the SSL cache.

Command Syntax and Usage
sslconnect
Displays the number of completed SSL client connections for the current VPN.
revocation
Displays the number of revoked client certificates.
cipherrewr
Displays the number of HTTP weak cipher rewrites.
http_redir
Displays the number of HTTP redirect rewrites.
becnctfail
Displays the number of failed connections to backend servers.
tps
Displays the number of SSL transactions per second for the specified VPN, as performed on all AVG devices in the cluster.
tpshisto
Displays histograms of the number of SSL transactions per second for the specified VPN on all AVG devices in the cluster.
clihisto
Displays histograms of data throughput in bytes per second from clients for the specified VPN, as performed on all AVG devices in the cluster.
srvhisto
Displays histograms of data throughput in bytes per second from backend servers for the specified VPN, as performed on all AVG devices in the cluster.
dump
Displays all statistics for the VPN, except the histograms.

/stats/sslstats/server <number> Cluster Wide SSL Statistics for Server Menu

```
[Cluster Wide SSL Stats for Server 1 Menu]
accept     - SSL accept
handshakeg - SSL handshakes completed
cachemisse - SSL cache misses
```

```
cachetimeo - SSL cache timeout
cachefull  - SSL cache full
cachehits  - SSL cache hits
sslconnect - SSL connects
revocation - Client cert revocations
cipherrewr - HTTP weak cipher rewrites
http_redir - HTTP redirect rewrites
becnctfail - Failed backend server connects
tps  - SSL transactions/sec
tpshisto   - Cluster wide TPS histograms for this server
clihisto   - Cluster wide client byte/s histos for this server
srvhisto   - Cluster wide server data byte/s histos for this server
dump       - Print all stats except histograms
```

The Cluster Wide SSL Statistics Server menu is used for viewing various statistics for a virtual SSL server, specified by its index number. The figures presented are accumulated from all AVG devices in the cluster, but specific for the selected virtual SSL server.

Table 8: Cluster Wide SSL Statistics for Server Menu Options (/stats/sslstats/server)

Command Syntax and Usage
accept Displays the number of initiated SSL client connections on the current virtual SSL server.
handshakeg Displays the number of successfully completed SSL handshakes on the current virtual SSL server. The number of failed SSL handshakes equals the value for **SSL accept** , minus the combined values for **SSL handshakes completed** and **Number of currently active request sessions**. You can view the values mentioned above by using the **/stats/dump** command.
cachemisse Displays the number of times clients have made requests to reuse a particular session ID, and that session ID was not found in the SSL cache. If there is a high number of cache misses in combination with a high value for **cachefull**, you may consider increasing the SSL cache size of the virtual SSL server, using the **/cfg/ssl /server #/ssl/cachesize** command. The default SSL cache size is 4000 items. If there is a high number of cache misses in combination with a low value for **cachefull**, you may consider increasing the cachettl value, using the **/cfg/ssl/server #/ssl /cachettl** command. The default SSL cache timeout value is 5 minutes.
cachetimeo Displays the number of reuse attempts on SSL sessions still in the cache, and whose timeouts were initiated.

Command Syntax and Usage
If there is a high number of cache timeouts, you may consider increasing the **cachettl** value for the virtual SSL server, using the **/cfg/ssl/server #/ssl/cachettl** command. The default SSL cache timeout value is 5 minutes.
cachefull
Displays the number of times when a new client session could not be cached due to the cache being full. If the **cachefull** value is high, you may consider increasing the SSL cache size of the virtual SSL server.
cachehits
Displays the number of times clients have made requests to reuse a particular session ID, and that session ID was found in the SSL cache.
sslconnect
Displays the number of completed SSL client connections on the current virtual SSL server.
revocation
Displays the number of revoked client certificates.
cipherrewr
Displays the number of HTTP weak cipher rewrites.
http_redir
Displays the number of HTTP redirect rewrites.
becnctfail
Displays the number of failed connections to backend servers.
tps
Displays the number of SSL transactions per second for the specified virtual SSL server, as performed on all AVG devices in the cluster.
tpshisto
Displays histograms of the number of SSL transactions per second, as performed by the specified virtual SSL server on all AVG devices in the cluster.
clihisto
Displays histograms of data throughput in bytes per second from clients to the specified virtual SSL server, as performed on all AVG devices in the cluster.
srvhisto
Displays histograms of data throughput in bytes per second from backend servers to the specified virtual SSL server, as performed on all AVG devices in the cluster.

Command Syntax and Usage	
dump	
	Displays all SSL statistics for the current virtual SSL server, except the histograms. For a sample screen output, see /stats/sslstats/server <number> /dump Cluster-Wide SSL Statistics for Server on page 58.

/stats/sslstats/server <number> /dump Cluster-Wide SSL Statistics for Server

```
Cluster wide SSL Stats for Server 1001:
10.1.82.146:443 SSL accept = 90
10.1.82.146:443 SSL handshakes completed = 90
10.1.82.146:443 SSL cache misses = 9
10.1.82.146:443 SSL cache timeout = 1
10.1.82.146:443 SSL cache full = 0
10.1.82.146:443 SSL cache hits = 78
10.1.82.146:443 SSL connects = 0
10.1.82.146:443 Client cert revocations = 0
10.1.82.146:443 HTTP weak cipher rewrites = 0
10.1.82.146:443       HTTP redirect rewrites = 2
10.1.82.146:443 Failed backend server connects = 0
10.1.82.146:443 SSL transactions/sec = 0
```

The output shows all SSL statistics for the current virtual SSL server, except the histograms.

/stats/sslstats/local Local SSL Statistics Menu

```
[Local SSL Statistics Menu]
      isdhost    - ISD local SSL server statistics menu
      overview   - Overview of isdhost local statistics
      tpshisto   - ISD local TPS histograms for all servers/ISDs
      clihisto   - ISD local client byte/s histos for all servers/ISDs
      srvhisto   - ISD local server data byte/s histos for all servers/ISDs
      license    - ISD local license statistics
      dump       - Dump all information
```

The Local Statistics menu is used for viewing histograms of SSL transactions per second, received client data and received backend server data (in bytes per second). Values are presented for each virtual SSL server, on a per AVG device basis. You can therefore easily compare the performance of a particular virtual SSL server on different AVG devices in the cluster.

The Local Statistics menu is also used for accessing the Single iSD Stats menu, in which you can view the same histograms as in the Local Statistics menu, with the difference that the histograms only pertain to a single AVG device (specified by host index number).

The **dump** command in the Local Statistics menu displays a number of statistics, where most of them relate to various SSL properties for incoming client connections. These statistics are

presented for each virtual SSL server, on a per AVG device basis. Information related to the health check status (of backend servers) and pool status may also be displayed, depending on your virtual SSL server configuration. This information is also displayed on a per AVG device basis, because each AVG performs its own health checking of configured backend servers independently from other AVGs in the cluster.

Histograms are not included in the output when running the **dump** command.

Table 9: Local Statistics Menu Options (/stats/sslstats/local)

Command Syntax and Usage
isdhost < AVG *host by index number (1-256)*> Displays the Single ISD Stats menu, after you have specified the index number of an AVG host in the cluster. To view menu options, see /stats/sslstats/local/isdhost <number> Single iSD Statistics Menu on page 60. To view information about host index numbers for all AVG hosts in the cluster, use the **/cfg/sys/cur** command.
overview Displays the total number of completed request sessions for each virtual SSL server on a per AVG device basis. An overview of the health check status of backend servers and the pool status may also be displayed, depending on your virtual SSL server configuration.
tpshisto Displays histograms of the number of SSL transactions per second, as performed by each virtual SSL server on a per AVG device basis.
clihisto Displays histograms of data throughput in bytes per second from clients to each virtual SSL server, on a per AVG device basis.
srvhisto Displays histograms of data throughput in bytes per second from backend servers to each virtual SSL server, on a per AVG device basis.
license Displays information about the number of times the tps license has reached the limit.
dump Displays various SSL statistics for incoming client connections, as well as HTTP-related statistics. The statistics are presented for each virtual SSL server, on a per AVG device basis. Histograms are not included in the output. For a sample screen output, see /stats/sslstats/local/dump Local SSL Statistics on page 60.

/stats/sslstats/local/dump Local SSL Statistics

```
Local SSL Statistics:
Single ISD SSL Stats 1:
Single ISD SSL Stats for Server 1:
10.1.82.146:80  SSL accept = 0
10.1.82.146:80  SSL handshakes completed = 0
10.1.82.146:80  SSL cache misses = 0
10.1.82.146:80  SSL cache timeout = 0
10.1.82.146:80  SSL cache full = 0
10.1.82.146:80  SSL cache hits = 0
10.1.82.146:80  SSL connects = 0
10.1.82.146:80  Client cert revocations = 0
10.1.82.146:80  HTTP weak cipher rewrites = 0
10.1.82.146:80  HTTP redirect rewrites = 0
10.1.82.146:80  Failed backend server connects = 0
10.1.82.146:80  SSL transactions/sec = 0
Single ISD SSL Stats for Server 1001:
10.1.82.146:443 SSL accept = 90
10.1.82.146:443 SSL handshakes completed = 90
10.1.82.146:443 SSL cache misses = 9
10.1.82.146:443 SSL cache timeout = 1
10.1.82.146:443 SSL cache full = 0
10.1.82.146:443 SSL cache hits = 78
10.1.82.146:443 SSL connects = 0
10.1.82.146:443 Client cert revocations = 0
10.1.82.146:443 HTTP weak cipher rewrites = 0
10.1.82.146:443 HTTP redirect rewrites = 2
10.1.82.146:443 Failed backend server connects = 0
10.1.82.146:443 SSL transactions/sec = 0
```

The output shows all SSL statistics per VPN Gateway, except the histograms. The statistics are presented per virtual SSL server for each VPN Gateway. Histograms are not included in the output.

The sample output above shows two virtual SSL servers. The server with number 1 is a virtual SSL server configured under **/cfg/ssl**. These servers are numbered from 1 and up. The server with number 1001 is a portal server, configured under **/cfg/vpn**. Server numbers assigned to portal servers start with 1001.

/stats/sslstats/local/isdhost <number> Single iSD Statistics Menu

```
[Single ISD SSL Stats 1 Menu]
      server     - ISD local SSL server stats
      tpshisto   - ISD local TPS histograms for all servers
      clihisto   - ISD local client byte/s histograms for all servers
      srvhisto   - ISD local server byte/s histograms for all servers
      dump       - Dump all information
```

The Single iSD Statistics menu is used for viewing histograms of SSL transactions per second, received client data, and received backend server data (in bytes per second). Values are

presented for each virtual SSL server in the cluster, as performed on a single AVG device (specified by host index number when you enter the Single iSD Statistics menu).

The Single iSD Statistics menu is also used for accessing the Single iSD Stats for Server menu, in which you can view various statistics related to one specific virtual SSL server as performed on the currently selected AVG host.

The **dump** command in the Single iSD Statistics menu displays a number of statistics where most of them are related to various SSL properties for incoming client connections for each virtual SSL server individually, as performed on the selected individual VPN Gateway. Histograms are not included in the output when running the **dump** command.

Table 10: Single iSD Statistics Menu Options (/stats/sslstats/local/isdhost)

Command Syntax and Usage
server *<virtual SSL server number>* Displays the Single iSD Stats for Server # menu. To view menu options, see /stats/sslstats/local/isdhost <number> /server <number> Single ISD SSL Statistics for Virtual SSL Server Menu on page 61.
tpshisto Displays histograms of the number of SSL transactions per second for each virtual SSL server, as performed on the currently specified VPN Gateway.
clihisto Displays histograms of data throughput in bytes per second from clients to each virtual SSL server, as performed on the currently specified VPN Gateway.
srvhisto Displays histograms of data throughput in bytes per second from backend servers to each virtual SSL server, as performed on the currently specified VPN Gateway.
dump Displays various SSL properties for incoming client connections, as well as HTTP-related statistics. The statistics are presented for each virtual SSL server in the cluster, but where the figures relate only to the currently specified VPN Gateway. Histograms are not included in the output.

/stats/sslstats/local/isdhost <number> /server <number> Single ISD SSL Statistics for Virtual SSL Server Menu

```
[Single ISD SSL Stats for Server 1 Menu]
```

```
healthchec - Display health check status for all loadbalanced RIPs
poolstatus - Pool status and statistics
accept     - SSL accept
handshakeg - SSL handshakes completed
cachemisse - SSL cache misses
cachetimeo - SSL cache timeout
cachefull  - SSL cache full
cachehits  - SSL cache hits
sslconnect - SSL connects
revocation - Client cert revocations
cipherrewr - HTTP weak cipher rewrites
http_redir - HTTP redirect rewrites
becnctfail - Failed backend server connects
tps  - SSL transactions/sec
tpshisto   - isdhost local TPS histograms for this server
clihisto   - isdhost local client byte/s histos for this server
srvhisto   - isdhost local server data byte/s histos for this server
dump       - Dump all information
```

The Single iSD Stats for Server # menu is used for viewing the pool status for backend servers that are load balanced by the specified virtual SSL server. The health check status of backend servers can also be displayed. Remember that each AVG device (or host) performs its own health checks of configured backend servers, which makes the status information unique for the specified VPN Gateway.

Other statistics can also be displayed, such as statistics related to SSL properties for incoming client connections handled by the specified virtual SSL server on the currently selected VPN Gateway. The values are unique for the selected VPN Gateway, because the figures depend on the Application Switch load balancing configuration of the server group in which the VPN Gateway resides.

The **dump** command will display all statistics available through the individual commands in the menu, except the health check status, pool status, and histograms.

Table 11: Single iSD Statistics Server Menu Options (/stats/sslstats/local/isdhost/server)

Command Syntax and Usage
healthchec Displays the health check status for the backend servers that are load balanced by the current virtual SSL server. Because each AVG device (or host) performs its own health checks of configured backend servers, the displayed health check status information is specific not only for the selected virtual SSL server, but also for the selected AVG host. The following health check properties are displayed: • `BE:` Backend servers by index number. • `RIP:` Load balanced backend servers listed by IP address and TCP port. • `UP:` Lists the current status of backend servers as `up` or `down`, where backend servers that passed the health check are indicated as `up`.

Command Syntax and Usage
• EXEC: Indicates whether a health check is currently being performed on a backend server. • FAILS: Indicates the number of times a health check has failed. For more information about script-based health checks, see the "Script-Based Health Checks" chapter in the *Application Guide for SSL Acceleration*. • REASON: States the reason, in clear text, for why a health check failed. **Note:** If you have enabled load balancing of configured backend servers and set the health check method to `none`, all backend servers will at all times be considered `up`. Failed connections to backend servers are still logged (as a total) and can be viewed using the **`/stats/sslstats/server #/becnctfail`** command. **Note:** If you have not added any backend servers to the system configuration, the IP address specified as the Real Server IP (RIP) for the current virtual SSL server is listed under the RIP column. When using the AVG together with an Application Switch, the RIP typically corresponds to 0.0.0.0. By specifying 0.0.0.0 as the Real Server IP address, the SSL server is instructed to use the destination IP address (in the received packets) when initiating requests sent to the virtual server. Such a RIP configuration ensures that requests initiated by the virtual SSL server always reach the correct Virtual Server IP address (as configured on the Application Switch), because the destination IP address in the received packets corresponds to the IP address of the virtual server. For a sample screen output, see /stats/sslstats/local/isdhost #/server #/ healthchec Single iSD Host SSL Server Healthcheck Command on page 66.
`poolstatus`
Displays pool status for the backend servers that are load balanced by the current virtual SSL server (where one pool is maintained for each backend server that passed the health check). Because each AVG device (or host) performs its own health checks of configured backend servers, the displayed pool status information is specific not only for the selected virtual SSL server, but also for the selected AVG host. The following pool status information is displayed: • BE: Backend servers by index number. • RIP: Backend servers (listed by IP address), for which a pool is maintained. • fds: File Descriptors. The number of server-side sockets that are currently in the pool. • sess: SSL sessions. The number of SSL sessions that are currently in the pool. A pooled SSL session can be reused when setting up a new server-side socket.

Command Syntax and Usage
• `poolcnct:` The number of server-side sockets in the pool that have been reused. • `!poolcnct:` The number of server-side sockets that have been set up without taking advantage of reusing an existing socket. **Note:** If you have not added any backend servers to the system configuration, the IP address specified as the Real Server IP (RIP) for the current virtual SSL server is listed under the RIP column. When using the AVG together with an Application Switch, the RIP typically corresponds to 0.0.0.0. By specifying 0.0.0.0 as the Real Server IP address, the SSL server is instructed to use the destination IP address (in the received packets) when initiating requests sent to the virtual server. Such a RIP configuration ensures that requests initiated by the virtual SSL server always reach the correct Virtual Server IP address (as configured on the Application Switch), because the destination IP address in the received packets corresponds to the IP address of the virtual server. For a sample screen output, see /stats/sslstats/local/isdhost #/server #/ poolstatus Single iSD Host SSL Server Poolstatus Command on page 66.
accept
Displays the number of initiated SSL client connections on the current virtual SSL server.
handshakeg
Displays the number of successfully completed SSL handshakes on the current virtual SSL server. To view the number of failed SSL handshakes, use the **/stats/dump** command. The number of failed SSL handshakes equals the value **SSL accept** , minus the combined values for **SSL handshakes completed** and the number of currently active request sessions.
cachemisse
Displays the number of times clients have made requests to reuse a particular session ID, and that session ID was not found in the SSL cache. If there is a high number of cache misses in combination with a high value for **cachefull**, you may consider increasing the SSL cache size of the virtual SSL server. To change the current SSL cache size, use the **/cfg/ssl/server** command, specify the appropriate virtual SSL server by index number, and then type the command **ssl/cachesize**. The default SSL cache size is 8000 items. If there is a high number of cache misses in combination with a low value for **cachefull**, you may consider increasing the **cachettl** value. To change the current cachettl value, use the **/cfg/ssl/server** command, specify the appropriate virtual SSL server by index number, and then type the command **ssl/cachettl**. The default SSL cache timeout value is 5 minutes.

Command Syntax and Usage
cachetimeo
Displays the number of reuse attempts on SSL sessions still in the cache, and whose timeouts were initiated. If there is a high number of cache timeouts, you may consider increasing the **cachettl** value for the virtual SSL server. To change the current **cachettl** value, use the **/cfg/ssl/server** command, specify the appropriate virtual SSL server by index number, and then type the command **ssl/cachettl**. For more information, see the **cachettl** command on cfg ssl server id ssl SSL Settings Configuration on page 94. The default SSL cache timeout value is 5 minutes.
cachefull
Displays the number of times when a new client session could not be cached due to the cache being full. If the **cachefull** value is high, you may consider increasing the SSL cache size of the virtual SSL server.
cachehits
Displays the number of times clients have made requests to reuse a particular session ID, and that session ID was found in the SSL cache.
sslconnect
Displays the number of completed SSL client connections on the current virtual SSL server.
revocation
Displays the number of revoked client certificates.
cipherrewr
Displays the number of HTTP weak cipher rewrites.
http_redir
Displays the number of HTTP redirect rewrites.
becnctfail
Displays the number of failed connections to backend servers.
tps
Displays the number of SSL transactions per second as performed by the specified virtual SSL server on the currently selected VPN Gateway.
tpshisto
Displays histograms of the number of SSL transactions per second for the specified virtual SSL server, as performed on the currently selected VPN Gateway.
clihisto

Command Syntax and Usage
Displays histograms of data throughput in bytes per second from clients to the specified virtual SSL server, as performed on the currently selected VPN Gateway.
srvhisto
Displays histograms of data throughput in bytes per second from backend servers to the specified virtual SSL server, as performed on the currently selected VPN Gateway.
dump
Displays all statistics for the specified virtual SSL server on the currently selected VPN Gateway, except the health check status, pool status, and histograms.

/stats/sslstats/local/isdhost #/server #/healthchec Single iSD Host SSL Server Healthcheck Command

```
>> Single ISD SSL Stats for Server 1# healthchec

 Healthcheck status at ISD number '1'
BE     RIP          UP     EXEC FAILS REASON
1          192.168.128.1:80     up no
```

/stats/sslstats/local/isdhost #/server #/poolstatus Single iSD Host SSL Server Poolstatus Command

```
>> Single ISD SSL Stats for Server 1# poolstatus

 Poolstatus at ISD number '1'
BE     RIP         fds    sess        poolcnct    !poolcnct
1          192.168.128.1:80     0     0          0          0
```

/stats/ipsec IPsec Statistics Menu

```
[IPSEC stats Menu]
      vpn        - Cluster IPSEC Server statistics
      local      - Local statistics for each isdhost
      clear      - Clear all ipsec statistics for all IPs
      activesess - Number of currently active ipsec User sessions
      totalsess  - Total completed ipsec User sessions
      failedsess - Total failed ipsec User sessions
      enctot     - Total encoded kBytes
      dectot     - Total decoded kBytes
      enc        - Encoded User kB/sec last minute
      boenc      - Encoded BO kB/sec last minute
      dec        - Decoded User kB/sec last minute
      bodec      - Decoded kB/sec last minute
      sesshisto  - Cluster-wide ipsec User session histograms for all VPNs
      enchisto   - Cluster-wide ipsec User encrypt histograms for all VPNs
      dechisto   - Cluster-wide ipsec User decrypt histograms for all VPNs
      boenchisto - Cluster-wide ipsec BO encrypt histograms for all VPNs
      bodechisto - Cluster-wide ipsec BO decrypt histograms for all VPNs
```

The IPsec Statistics menu is used for viewing performance statistics relating to IPsec sessions.

Note:

This menu is not available if the VPN Gateway software is run on the ASA 310 or ASA 410 hardware platforms.

Table 12: IPsec Statistics Menu Options (/stats/ipsec)

Command Syntax and Usage
vpn <*VPN ID*> Displays the Cluster Wide IPsec Statistics menu for the specified VPN. Press TAB following this command to view available VPN IDs. To view menu options see, /stats/ipsec/vpn <id> Cluster Wide IPsec Statistics for VPN Menu on page 69.
local Displays the Local Statistics menu. To view menu options see, /stats/ipsec/local Local IPsec Statistics Menu on page 71.
clear Resets all IPsec statistics to zero.
activesess Displays the number of currently active IPsec user sessions for all VPNs in the cluster.
totalsess

Command Syntax and Usage
Displays the total number of completed IPsec user sessions for all VPNs in the cluster. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
failedsess
Displays the number of failed IPsec user sessions for all VPNs in the cluster. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enctot
Displays the total number of encoded kBytes for all VPNs in the cluster. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
dectot
Displays the total number of decoded kBytes for all VPNs in the cluster. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enc
Displays the number of encoded kBytes per second during the last minute, for user tunnels in all VPNs in the cluster.
boenc
Displays the number of encoded kBytes per second during the last minute, for branch office tunnels in all VPNs in the cluster.
dec
Displays the number of decoded kBytes per second during the last minute, for user tunnels in all VPNs in the cluster.
bodec
Displays the number of decoded kBytes per second during the last minute, for branch office tunnels in all VPNs in the cluster.
sesshisto
Displays cluster wide IPsec session histograms for all VPNs. The histograms show the average number of sessions per minute, hour and day up to 31 days.
enchisto
Displays cluster wide IPsec encryption histograms for user tunnel sessions in all VPNs. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dechisto

Command Syntax and Usage
Displays cluster wide IPsec decryption histograms for user tunnel sessions in all VPNs. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
boenchisto
Displays cluster wide IPsec encryption histograms for branch office tunnels in all VPNs. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
bodechisto
Displays cluster wide IPsec decryption histograms for branch office tunnels in all VPNs. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.

/stats/ipsec/vpn <id> Cluster Wide IPsec Statistics for VPN Menu

```
[Cluster wide IPSEC Stats for VPN 1 Menu]
      activesess - Number of currently active ipsec User sessions
      totalsess  - Total completed ipsec User sessions
      failedsess - Total failed ipsec User sessions
      enctot     - Total encryped kBytes
      dectot     - Total decryped kBytes
      enc        - Encrypted User kB/sec last minute
      boenc      - Encrypted BO kB/sec last minute
      dec        - Decrypted User kB/sec last minute
      bodec      - Decrypted BO kB/sec last minute
      sesshisto  - cluster wide ipsec User sess histograms for this VPN
      enchisto   - cluster wide ipsec User encryption histograms for this VPN
      dechisto   - cluster wide ipsec User decryption histograms for this VPN
      boenchisto - cluster wide ipsec BO encryption histograms for this VPN
      bodechisto - cluster wide ipsec BO decryption histograms for this VPN
      dump       - Print all stats except histograms
```

The Cluster Wide IPsec Statistics for VPN menu is used for viewing IPsec session statistics for a specific VPN.

Table 13: Cluster Wide IPsec Statistics for VPN Menu Options (/stats/ipsec/vpn)

Command Syntax and Usage
activesess
Displays the number of currently active IPsec sessions for the selected VPN.
totalsess
Displays the total number of completed IPsec sessions for the selected VPN. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
failedsess
Displays the number of failed IPsec sessions for the selected VPN.

Command Syntax and Usage
The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enctot
Displays the total number of encoded kBytes for the selected VPN. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
dectot
Displays the total number of decoded kBytes for the selected VPN. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enc
Displays the number of encoded kBytes per second during the last minute, for user sessions in the selected VPN.
boenc
Displays the number of encoded kBytes per second during the last minute, for branch office tunnel sessions in the selected VPN.
dec
Displays the number of decoded kBytes per second during the last minute, for user sessions in the selected VPN.
bodec
Displays the number of decoded kBytes per second during the last minute, for branch office tunnel sessions in the selected VPN.
sesshisto
Displays cluster wide IPsec user session histograms for the selected VPN. The histograms show the average number of sessions per minute, hour and day up to 31 days.
enchisto
Displays cluster wide IPsec encryption histograms for user sessions in the selected VPN. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dechisto
Displays cluster wide IPsec decryption histograms for user sessions in the selected VPN. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
boenchisto

Command Syntax and Usage
Displays cluster wide IPsec encryption histograms for branch office tunnels in the selected VPN. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
bodechisto
Displays cluster wide IPsec decryption histograms for branch office tunnels in the selected VPN. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dump
Displays all IPsec statistics for the selected VPN, except the histograms. For a sample screen output, see /stats/ipsec/vpn <id> /dump Cluster-Wide IPsec Statistics for VPN on page 71.

/stats/ipsec/vpn <id> /dump Cluster-Wide IPsec Statistics for VPN

```
Cluster wide IPsec Stats for VPN 1:
VPN(1)    Active ipsec user sessions = 0
VPN(1)    Total ipsec user sessions = 0
VPN(1)    Total failed user sessions = 0
VPN(1)    Total encrypted kBytes = 0
VPN(1)    Total decrypted kBytes = 0
VPN(1)    Encrypt User kB/sec last minute = 0
VPN(1)          Encrypt BO kB/sec last minute = 0
VPN(1)          Decrypt User kB/sec last minute = 0
VPN(1)    Decrypt BO kB/sec last minute = 0
```

The output shows all IPsec statistics for the selected VPN, except the histograms.

/stats/ipsec/local Local IPsec Statistics Menu

```
[Local IPSEC Statistics Menu]
      isdhost    - ISD local  IPSEC server statistics menu
      sesshisto  - ISD local ipsec User session histograms for all VPNs/ISDs
      enchisto   - ISD local ipsec User encrypt histograms for all VPNs/ISDs
      dechisto   - ISD local ipsec User decrypt histograms for all VPNs/ISDs
      boenchisto - ISD local ipsec BO encrypt histograms for all VPNs/ISDs
      bodechisto - ISD local ipsec BO decrypt histograms for all VPNs/ISDs
      dump       - Dump all information
```

The Local IPsec Statistics menu is used for viewing IPsec statistics per VPN Gateway (iSD), if the cluster consists of several devices. For each VPN Gateway, the statistics are shown per VPN. Using the **isdhost** command, you can view statistics for specific VPN Gateways in the cluster.

Table 14: Local IPsec Statistics Menu Options (/stats/ipsec/local)

Command Syntax and Usage
isdhost Displays the Single ISD Statistics menu where you can view statistic information for a specified VPN Gateway. To view menu options, see /stats/ipsec/local/isdhost <number> Single iSD IPsec Statistics Menu on page 73.
sesshisto Displays IPsec session histograms for user tunnels per VPN Gateway. The histograms show the average number of sessions per minute, hour and day up to 31 days.
enchisto Displays IPsec encryption histograms for user tunnels per VPN Gateway. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dechisto Displays IPsec decryption histograms for user tunnels per VPN Gateway. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
boenchisto Displays IPsec encryption histograms for branch office tunnels per VPN Gateway. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
bodechisto Displays IPsec decryption histograms for branch office tunnels per VPN Gateway. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dump Displays all IPsec statistics per VPN Gateway and VPN, except the histograms. For a sample screen output, see /stats/ipsec/vpn <id> /dump Cluster-Wide IPsec Statistics for VPN on page 71.

/stats/ipsec/local/dump Single VPN Gateway IPsec Statistics

```
Local IPsec Statistics:
Single ISD IPSEC Stats 1:
ipsec_active_sess: 0
ipsec_total_sess: 0
```

```
ipsec_failed_sess: 0
ipsec_total_enc: 0
ipsec_total_dec: 0
ipsec_enc: 0
ipsec_bo_enc: 0
ipsec_dec: 0
ipsec_bo_dec: 0
Single ISD IPSEC Stats for VPN 1:
VPN(1)    Ipsec active sessions = 0
VPN(1)    Ipsec total sessions = 0
VPN(1)    Ipsec total failed sessions = 0
VPN(1)    Ipsec total encrypted kB = 0
VPN(1)    Ipsec total decrypted kB = 0
VPN(1)    Ipsec encode kb/sec last minute = 0
VPN(1)    Ipsec decode kb/sec last minute = 0
VPN(1)    Ipsec decode kb/sec last minute = 0
VPN(1)    Ipsec decode kb/sec last minute = 0
Single ISD IPSEC Stats for VPN 2:
VPN(2)    Ipsec active sessions = 0
VPN(2)    Ipsec total sessions = 0
VPN(2)    Ipsec total failed sessions = 0
VPN(2)    Ipsec total encrypted kB = 0
VPN(2)    Ipsec total decrypted kB = 0
VPN(2)    Ipsec decode kb/sec last minute = 0
VPN(1)    Ipsec decode kb/sec last minute = 0
VPN(1)    Ipsec decode kb/sec last minute = 0
VPN(1)    Ipsec decode kb/sec last minute = 0
```

The output shows all IPsec statistics per VPN Gateway and VPN, except the histograms.

/stats/ipsec/local/isdhost <number> Single iSD IPsec Statistics Menu

```
[Single ISD IPSEC Stats 1 Menu]
      vpn        - ISD local IPSEC server stats
      activesess - Locally active ipsec User sessions all VPNs
      totalsess  - Locally total ipsec User sessions all VPNs
      failedsess - Locally failed ipsec User sessions, all VPNs
      enctot     - Locally total ipsec encoded kBytes all VPNs
      dectot     - Locally total ipsec decoded kBytes all VPNs
      enc        - Locally ipsec User encoded kB/sec last minute all VPNs
      boenc      - Locally ipsec BO encoded kB/sec last minute all VPNs
      dec        - Locally ipsec User decoded kB/sec last minute all VPNs
      bodec      - Locally ipsec BO decoded kB/sec last minute all VPNs
      sesshisto  - ISD local ipsec User sess histograms for all VPNs
      enchisto   - ISD local ipsec User encrypt histograms for all VPNs
      dechisto   - ISD local ipsec User decrypt histograms for all VPNs
      boenchisto - ISD local ipsec BO encrypt histograms for all VPNs
      bodechisto - ISD local ipsec BO decrypt histograms for all VPNs
      dump       - Dump all information
```

The Single ISD IPsec Statistics menu is used for viewing IPsec statistics for a specific VPN Gateway (iSD), that is, the statistics do not relate to the whole cluster of VPN Gateways. The statistics are shown per VPN.

Table 15: Single ISD IPsec Statistics Menu Options (/stats/ipsec/local/isdhost)

Command Syntax and Usage
vpn Displays the Single ISD IPsec Statistics for VPN menu. To view menu options, see /stats/ipsec/local/isdhost <number> /vpn <id> Single iSD IPsec Statistics for VPN Menu on page 76.
activesess Displays the number of currently active IPsec user sessions for the selected VPN Gateway.
totalsess Displays the total number of completed IPsec user sessions for the selected VPN Gateway. The information includes all user sessions since the system was first started or since the statistics were last cleared using the **clear** command.
failedsess Displays the number of failed IPsec user sessions for the selected VPN Gateway. The information includes all user sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enctot Displays the total number of encoded kBytes for the selected VPN Gateway. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
dectot Displays the total number of decoded kBytes for the selected VPN Gateway. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enc Displays the number of encoded kBytes per second during the last minute, for user tunnels on the selected VPN Gateway.
boenc Displays the number of encoded kBytes per second during the last minute, for branch office tunnels on the selected VPN Gateway.
dec Displays the number of decoded kBytes per second during the last minute, for user tunnels on the selected VPN Gateway.
bodec

Command Syntax and Usage
Displays the number of decoded kBytes per second during the last minute, for branch office tunnels on the selected VPN Gateway.
sesshisto
Displays IPsec session histograms for the selected VPN Gateway. The histograms show the average number of sessions per minute, hour and day up to 31 days.
enchisto
Displays IPsec encryption histograms for user tunnels in the selected VPN Gateway. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dechisto
Displays IPsec decryption histograms for user tunnels on the selected VPN Gateway. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
boenchisto
Displays IPsec encryption histograms for branch office tunnels in the selected VPN Gateway. The histograms show the average encryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
bodechisto
Displays IPsec decryption histograms for branch office tunnels on the selected VPN Gateway. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dump
Displays all IPsec statistics for the selected VPN Gateway, except the histograms.

/stats/ipsec/local/isdhost <number> /vpn <id> Single iSD IPsec Statistics for VPN Menu

```
------------------------------------------------------------
[Single ISD IPSEC Stats for VPN 1 Menu]
      activesess - Active ipsec sessions
      totalsess  - Total ipsec sessions
      failedsess - Total failed ipsec sessions
      enctot     - Total ipsec encrypted kBytes
      dectot     - Total ipsec decrypted kBytes
      enc        - ipsec encoded User kB/s last minute
      boenc      - ipsec encoded BO kB/s last minute
      dec        - ipsec decoded kB/s last minute
      bodec      - ipsec decoded BO kB/s last minute
      sesshisto  - isdhost local ipsec User sessions histograms for this VPN
      enchisto   - isdhost local ipsec User encrypt histograms for this VPN
      dechisto   - isdhost local ipsec User decrypt histograms for this VPN
      boenchisto - isdhost local ipsec BO encrypt histograms for this VPN
      bodechisto - isdhost local ipsec BO decrypt histograms for this VPN
      dump       - Dump all information
```

The Single ISD IPsec Statistics for VPN menu is used for viewing IPsec statistics for a specific VPN on the selected VPN Gateway (iSD).

Table 16: Single ISD IPsec Statistics for VPN Menu Options (/stats/ipsec/local/isdhost/vpn)

Command Syntax and Usage
activesess Displays the number of currently active IPsec sessions for the selected VPN Gateway and VPN.
totalsess Displays the total number of completed IPsec sessions for the selected VPN Gateway and VPN. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
failedsess Displays the number of failed IPsec sessions for the selected VPN Gateway and VPN. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enctot Displays the total number of encoded kBytes for the selected VPN Gateway and VPN. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
dectot

Command Syntax and Usage
Displays the total number of decoded kBytes for the selected VPN Gateway and VPN. The information includes all sessions since the system was first started or since the statistics were last cleared using the **clear** command.
enc
Displays the number of encoded kBytes per second during the last minute, for user tunnels on the selected VPN Gateway and VPN.
boenc
Displays the number of encoded kBytes per second during the last minute, for branch office tunnels on the selected VPN Gateway and VPN.
dec
Displays the number of decoded kBytes per second during the last minute, for user tunnels on the selected VPN Gateway and VPN.
bodec
Displays the number of decoded kBytes per second during the last minute, for branch office tunnels on the selected VPN Gateway and VPN.
sesshisto
Displays IPsec session histograms for the selected VPN Gateway and VPN.
enchisto
Displays IPsec encryption histograms for user tunnels on the selected VPN Gateway and VPN. The histograms show the average number of sessions per minute, hour and day up to 31 days.
dechisto
Displays IPsec decryption histograms for user tunnels on the selected VPN Gateway and VPN. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
boenchisto
Displays IPsec encryption histograms for branch office tunnels on the selected VPN Gateway and VPN. The histograms show the average number of sessions per minute, hour and day up to 31 days.
bodechisto
Displays IPsec decryption histograms for branch office tunnels on the selected VPN Gateway and VPN. The histograms show the average decryption times in kBytes per second. The information is shown per minute, hour and day up to 31 days.
dump

Command Syntax and Usage
Displays all statistics for the selected VPN Gateway and VPN, except the histograms. For a sample screen output, see /stats/ipsec/local/isdhost <number> /vpn <id> / dump Single VPN Gateway IPsec Statistics for VPN on page 78.

/stats/ipsec/local/isdhost <number> /vpn <id> /dump Single VPN Gateway IPsec Statistics for VPN

```
Single ISD IPSEC Stats for VPN 1:
VPN(1)     Ipsec active sessions = 0
VPN(1)     Ipsec total sessions = 0
VPN(1)     Ipsec total failed sessions = 0
VPN(1)     Ipsec total encrypted kB = 0
VPN(1)     Ipsec total decrypted kB = 0
VPN(1)           Ipsec encode kb/sec last minute = 0
VPN(1)     Ipsec decode kb/sec last minute = 0
```

The output shows all IPsec statistics for the selected VPN Gateway and VPN, except the histograms.

/stats/aaa AAA Statistics Menu

```
[AAA Statistics Menu]
      total      - Cluster-wide authentication statistics (per VPN)
      isdhost    - ISD local authentication statistics (per VPN)
      dump       - Dump all information
```

The AAA Statistics menu is used for viewing authentication statistics related to the AVG cluster as a whole, or to one specific VPN Gateway in the cluster.

The number of accepted and rejected authentication requests of VPN users are listed for each configured authentication method and authentication server. The remote authentication servers are listed by IP address and TCP port number.

Note that authentication statistics for all servers that are configured in the AVG cluster are displayed, and not only for the servers that are included in the authentication order scheme (by using the **`/cfg/vpn <id>/aaa/authorder`** command). If the statistics for a certain authentication method always comes down to a row with zeroes, this might be due to the fact that the method is not included in the authentication order scheme.

Table 17: AAA Statistics Menu Options (/stats/aaa)

Command Syntax and Usage
total Displays the total authentication statistics for all VPN Gateways in the cluster since the system was started.
isdhost <*host id*> <*VPN ID*> Displays the authentication statistics for the specified VPN Gateway and VPN. To view authentication statistics for all VPNs, enter 0 when prompted for VPN ID.
dump Dumps all authentication statistics in the CLI, that is, the total statistics and statistics sorted per VPN Gateway. For a sample screen output, see /stats/aaa/dump Accept/Reject Statistics per Authentication Method and VPN on page 79.

/stats/aaa/dump Accept/Reject Statistics per Authentication Method and VPN

```
>> AAA
Statistics#
dump

RADIUS          VPN             Accepted        Rejected        Time
Servers                                                         Out

192.168.128     1               8               1               0
.1:1812

10.1.0.10:18    2               6               0               0
12

Local DB        VPN             Accepted        Rejected

-----------------------
-----------------------
-----------------------
-----------------------
-----------------------
-----------------------
-----------------------
-----------------------
-----------------------
--
```

```
                1               0               0
                2               0               0
                3               0               0
                4               7               3
Licenses        VPN             Accepted        Rejected
----------------------
----------------------
----------------------
----------------------
----------------------
----------------------
----------------------
----------------------
----------------------
--
SSL             1               0               0
Vdesk           1               0               0
SPIKE           1               0               0
IPSEC           1               0               0
SSL             2               0               0
Vdesk           2               0               0
SPIKE           2               0               0
IPSEC           2               0               0
SSL             3               0               0
Vdesk           3               0               0
SPIKE           3               0               0
IPSEC           3               0               0
```

The first part of the output shows accepted/rejected connections to configured authentication servers. In the preceding example, VPNs 1 and 2 are both configured with RADIUS authentication, AVG local database authentication and client certificate authentication. Rejections occur for example when the user submits the wrong password. For remote authentication methods (for example RADIUS, LDAP and NTLM), the number of times an authentication request has timed out on a specific server is listed as well.

Under `Licenses`, the sum of `accepted` connections are presented per license type and VPN. Authentication server rejections are not included. In the preceding example, for VPN 1, there are 8 accepted connections to the RADIUS server and 4 to the local database. That makes a total of 12 accepted connections. Of those 12 connections, 10 are displayed under Accepted

and 2 under `Rejected`. This means that only 10 concurrent users are allocated to VPN 1. The figure under `Rejected` refers to connections exceeding the allowed number of concurrent users.

/cfg Configuration Menu

The Configuration menu is used for performing SSL and system-wide configuration, as well as for saving and restoring AVG configurations to and from a TFTP, FTP, SCP or SFTP server.

```
[Configuration Menu]
      ssl         - SSL offload menu
      cert        - Certificate menu
      vpn         - VPN menu
      test        - Create test vpn, portal and certificate
      quick       - Quick vpn setup wizard
      sys         - System-wide parameter menu
      lang        - Language support
      bwm         - Bandwidth management menu
      log         - logging system menu
      ptcfg       - Backup configuration to TFTP/FTP/SCP/SFTP server
      gtcfg       - Restore configuration from TFTP/FTP/SCP/SFTP server
      dump        - Dump configuration on screen for copy-and-paste
```

Table 18: Configuration Menu Options (/cfg)

Command Syntax and Usage
ssl Displays the SSL offload menu. To view menu options, see /cfg/ssl SSL Menu on page 86.
cert <*certificate index number*> Displays the Certificate menu, after you have typed the index number of an existing certificate or a new certificate. To view menu options, see /cfg/cert <id> Certificate Management Configuration on page 137.
vpn Displays the VPN menu. To view menu options, see /cfg/vpn <id> VPN Menu on page 146.
test Lets you run a wizard for creating a testVPN with the next available VPN ID. You will be prompted the following information: • Portal IP address for test portal. Used by the remote user to connect to the VPN. • Certificate. If you do not select an existing certificate, the system creates a test certificate with the next available certificate number. • User name and password for a test user. • IPsec. If your hardware model supports IPsec you will also have the option to enable IPsec, configure group authentication (including shared secret) and an IP address

Command Syntax and Usage
range to be used for unencrypted connections between the VPN Gateway and destination hosts. You can read more about IPsec in the "Transparent Mode" chapter in the *Application Guide for VPN*. • Net Direct. Lets you configure the VPN Gateway to allow use with the Net Direct client (SSL VPN client downloadable from Portal). If an IP address range has not yet been configured you will be prompted for this. You can read more about the Net Direct client in the "Net Direct" chapter in the *Application Guide for VPN*. The system configures the VPN to use local database authentication, adds the test user to the local database and creates a group called `test` with access to all networks, services and paths. The test user to is mapped to the `test` group. An empty linkset called `base-links` is created and mapped to the `test` group. If you create VPN using the **`/cfg/test`** command, the standalone mode is set to on by default.
`quick`
Lets you run a wizard for creating a sharp VPN with the next available VPN ID. You will be prompted the following information: • Portal IP address. Used by the remote user to connect to the VPN. • Name of VPN. Lets you enter a name for the VPN, for example My VPN. • VPN used with Alteon switch yes/no. Choose **`yes`** if an Application Switch (formerly Alteon Application Switch) is connected to the VPN Gateway, otherwise choose **`no`** . If set to **`no`** , the portal server will be set to standalone mode. • Which port number the Portal should listen to. The default value is 443 (https). • Support for short DNS names. Lets the remote user access hosts in the specified domain by using short names, for example `inside` instead of `inside.example.com`. • Certificate. Lets you use an existing certificate or paste a new certificate. • Chain certificate. Asks whether or not a chain certificate is needed and lets you use an existing certificate as the chain certificate or paste a new chain certificate. • HTTP to HTTPS redirect service. Automatically redirects requests made with http to the proper https server configured for the VPN, e.g. http://vpn.example.com gets redirected to https://vpn.example.com. • Default services. Creates a number of service definitions that can later be used to limit access to specific services (for example FTP, HTTP, SMTP and so on). • Trusted account. User name and password for a test user. • IPsec. If your hardware model supports IPsec you will also have the option to enable IPsec for user tunnels, configure group authentication (including shared secret) and an IP address range to be used for unencrypted connections between the VPN Gateway and destination hosts. You can read more about IPsec in the "Transparent Mode" chapter in the *Application Guide for VPN*. • Net Direct. Lets you configure the VPN Gateway to allow use with the Net Direct client (SSL VPN client downloadable from Portal). If an IP address range has not

Command Syntax and Usage
yet been configured you will be prompted for this. You can read more about the Net Direct client in the "Net Direct" chapter in the *Application Guide for VPN*. The system configures the VPN to use local database authentication, adds the test user to the local database and creates a group called `trusted` with access to all networks, services and paths. The test user to is mapped to the `trusted` group. An empty linkset called `base-links` is created and mapped to the `trusted` group.
sys
Displays the System Configuration menu. To view menu options, see /cfg/sys System Configuration on page 408.
lang
Displays the Language Support menu. To view menu options, see /cfg/lang Language Support Configuration on page 449.
bwm
Displays Bandwidth Management menu. To view menu options, see /cfg/bwm Bandwidth Management on page 450.
log
A logging system is used to cache the logging information in the internal buffer. This allows network to collect and access the logging information.
ptcfg *<method (TFTP/FTP/SCP/SFTP)> <server host name or IP address> <destination file name> <password phrase> <FTP user name and password> (if applicable)>*
Saves the current configuration, including private keys and certificates, to a TFTP/FTP/SCP/SFTP server. The configuration can later be restored by using the **gtcfg** command. You are required to specify a password phrase before the information is sent to the server. If you restore the configuration by using the **gtcfg** command, you will be prompted for the password phrase you have specified. The password phrase is used to protect the private keys in the configuration. **Note:** If you have fully separated the Administrator user role from the Certificate Administrator user role, the export passphrase defined by the certificate administrator is used to protect the private keys in the configuration—transparently to the user. When a configuration backup is restored by using the **gtcfg** command, the certificate administrator must enter the correct passphrase. For more information on separating the Administrator user role from the Certificate Administrator user role, see the "Adding a New User" section in the "Managing Users and Groups" chapter in the *User's Guide*.

Command Syntax and Usage
Note: When using the **ptcfg** command on an ASA FIPS, private keys are encrypted using the wrap key that was generated when the first HSM card in the cluster was initialized.
gtcfg *<method (TFTP/FTP/SCP/SFTP)> <server host name or IP address> <file name> <FTP user name and password (if applicable)> <password phrase>*
Restores a configuration, including private keys and certificates, from a TFTP/FTP/SCP/SFTP server. You need to provide the password phrase you specified when saving the configuration to the server. **Note:** If you have fully separated the Administrator user role from the Certificate Administrator user role (by removing the admin user from the certadmin group), the certificate administrator must enter the passphrase that he or she defined by using the **/cfg/sys/user/caphrase** command.
dump
Dumps the current configuration on screen in a format that allows you to restore the configuration without downloading the configuration to a file server. Save the configuration to a text file by performing a copy-and-paste operation to a text editor. The configuration can later be restored by pasting the contents of the saved text file at any command prompt in the command line interface using the global **paste** command. When pasted, the content is batch processed by the VPN Gateway. To view the pending configuration changes resulting from the batch processing, use the **diff** command. To apply the configuration changes, use the **apply** command. If you choose to include private keys in the configuration dump, you are required to specify a password phrase. The password phrase you specify applies to all private keys. When restoring a configuration that includes private keys, use the global **paste** command. Before pasting the configuration, you will be prompted for the password phrase you have specified. **Note:** When using this command on an ASA FIPS machine, private keys are only displayed for client certificates. For a sample screen output, see CLI Dumps on page 465 ".

Viewing, Applying and Removing Changes

As you use the configuration menus to set AVG parameters, the configuration changes you make do not take effect immediately. All changes are considered "pending" until you explicitly apply them.

While configuration changes are in the pending state, you can do the following:

- View the pending changes
- Apply the pending changes
- Remove the pending changes

Viewing Pending Changes

You can view all pending configuration changes by using the **diff** command at the menu prompt.

```
>> # diff
```

If you have pending configuration changes when using the **exit** command to log out from the command line interface, you will be prompted to view the pending changes by using the **diff** command. You can then either apply the changes, or remove them.

Applying Pending Changes

To make your configuration changes active, you must apply them. To apply pending configuration changes, use the **apply** command at the menu prompt.

```
>> # apply
```

Removing Pending Changes

To remove your pending configuration changes before they have been applied, use the **revert** command at the menu prompt.

```
>> # revert
```

Note:

The **diff, apply**, and **revert** commands are global commands. Therefore, you can enter these commands at any menu prompt in the command line interface.

/cfg/ssl SSL Menu

```
[SSL Menu]
server     - SSL server menu
test - Create test server and certificate
quick- Quick server setup wizard
```

The SSL menu is used for configuring virtual SSL servers. There are also menu options for creating a test server and a test certificate.

Table 19: SSL Configuration Menu Options (/cfg/ssl)

Command Syntax and Usage
server *<virtual SSL server index number>* Displays the Server menu, after you have typed the index number of an existing virtual SSL server or a new server. To view menu options, see /cfg/ssl/server <id> SSL Server Configuration on page 88.
test Creates a test SSL server using the first available virtual SSL index number. The default name of the test server is `test_server` . A test certificate and key are also created for the test SSL server. When executing the **test** command, you are asked to specify the IP address of a virtual server (defined on the Application Switch). The virtual server you specify will then make use of the services the test SSL server provides (HTTPS offload by default). You also need to specify which type of test SSL server you want to create. Depending on the type you choose to create, you will be prompted for additional related information. Valid SSL server types include the following: • `generic:` When selecting the generic SSL server type, you only need to specify a virtual server IP address. A generic SSL server listens on port 443 (HTTPS) and runs in transparent proxy mode. Contents handled by a generic SSL server is treated as generic data and will not be parsed. • `http:` When selecting the HTTP SSL server type, you only need to specify a virtual server IP address. A HTTP server shares many of its characteristics with the generic server type, but content is parsed as HTTP requests and responses. This paves the way for using a number of HTTP configuration options on the non-encrypted contents. For each of the preceding SSL server types, you have the option to use an existing certificate (if available), identified by the certificate index number, or create a test certificate.> For more information on the characteristics and capabilities of the respective server type, see the **type** command.
quick

Command Syntax and Usage

Lets you run a wizard for creating a sharp SSL server with he next available server ID. Before using the wizard, you must have obtained a server certificate in the PEM format that the virtual SSL server can use.
Note that even if the wizard provides an easy way to create and configure a virtual SSL server, you still must configure the Application Switch accordingly. The extent of configuration changes to filters and so on. needed on the Application Switch depend on your current setup and services. For detailed examples of virtual SSL server implementations in conjunction with an Application Switch, see the *Application Guide* for SSL Acceleration.
The VPN Gateway can also operate in standalone mode, that is, without being connected to an Application Switch. For configuration examples, see the "Standalone Web Server Accelerator" chapter in the *Application Guide for SSL Acceleration*.
You will be prompted the following information:

- Type of server. Lets you specify the type of server, that is, generic or http. For example, to create a server for HTTPS offload purposes, select http. When the SSL server type is set to HTTP, the virtual SSL server is automatically configured to use built-in features such as automatic SSL redirect and the adding of extra headers. For more information about these advanced HTTP-specific features, see the **`/cfg/ssl/server #/http`** command.
- IP address of SSL server. Lets you specify the IP address of an existing virtual server on the Application Switch to bind the HTTP virtual SSL server to that virtual server.
- Which port number the server should listen to. The default value is 443 (https) which is used for HTTPS offload purposes. To set up the virtual SSL server to handle IMAPS for example, set the listen TCP port to 993.
- Real server IP. Sets the IP address of the real server to which the virtual SSL server should connect when initiating requests. When using the VPN Gateway with an Application Switch, the real server IP address (RIP) should be the set to 0.0.0.0 (the default setting).
- Real server port. Defines the TCP port to which the virtual SSL server connects. When setting up a virtual SSL server for HTTPS offload purposes, the default real server port is 81. The virtual SSL server will use this port to send and receive decrypted HTTP information to and from the real web servers. The real Web servers must also be configured to listen for AVG traffic on port 81. For security reasons, it is also important to define a filter on the Application Switch that blocks all incoming client traffic destined for port 81.
- Should the site be password-protected (yes/no). If you choose yes here, a login window will be displayed when the user connects to the HTTP server. The login feature is on top of the SSL encryption, which makes it safe to enter user name and password. For user authentication, you will be prompted to select an existing VPN (if any). The authentication scheme adhering to this VPN will then be used.
- Is the real server an Outlook Web Access server (yes/no). Enabling this setting corresponds to enabling the `addfront` setting on the `/cfg/ssl/server #/http` menu.

Command Syntax and Usage
• Certificate. Lets you use an existing certificate or paste a new certificate. If you wish to use a certificate already present in the configuration, choose the desired certificate by entering the corresponding number, otherwise choose no. In this case you will be prompted to paste the certificate you want the virtual SSL server to use. • Chain certificate. If the server certificate you just added is a chain certificate, add your chain certificate(s) as well. You need to repeat the pasting of chain certificates until the root CA certificate has been added. This constructs the server certificate chain, which is sent to the client's browser in addition to the server certificate. When you have added your root CA certificate, answer no to the question if you require (additional) chain certificates.

/cfg/ssl/server <id> SSL Server Configuration

```
[Server 1 Menu]
      name       - Set server name
      vips       - Set IP addr(s) of server
      standalone - Set standalone mode
      port       - Set listen port of server
      rip        - Set real server IP addr
      rport      - Set real server port
      type       - Set type (generic/http/socks)
      dnsname    - Set DNS name of server
      proxy      - Set transparent proxy mode (on/off)
      trace      - Traffic trace menu
      ssl        - SSL settings menu
      tcp        - TCP endpoint settings menu
      http       - HTTP settings menu
      dns        - DNS settings menu
      socks      - Socks settings menu
      adv        - Advanced settings menu
      del        - Remove virtual server
      ena        - Enable virtual server
      dis        - Disable virtual server
```

The SSL Server menu is used for configuring various attributes of a particular virtual SSL server. The number of items available in the menu will vary according to the virtual SSL server type (generic, http or socks). When accessing the SSL Server menu, you are requested to specify the index number of the virtual SSL server you want to work with. To view information about all configured SSL servers, use the **/info/servers** command.

Table 20: SSL Server Configuration Menu Options (/cfg/ssl/server)

Command Syntax and Usage
name <*SSL server name*> Assigns a name to the virtual SSL server. The assigned name is mainly for your own reference. "" is the default value. You cannot enter only numerals as server name.
vips <*virtual server IP addresses separated by comma*> Sets the virtual server IP address (on the Application Switch), to which the virtual SSL server is mapped. For example: 10,127,232,48. If the VPN Gateway is used without a Application Switch (standalone mode), several IP addresses can be specified to create a solution where two or more VPN Gateways in a cluster are load-balanced by the DNS server. For configuration examples in standalone mode, see the "Stand-alone Web Server Accelerator" chapter in the *Application Guide for SSL Acceleration*.
standalone on|off • **on:** When set to **on**, the VPN Gateway operates in standalone mode, that is, it is not connected to an Application Switch. Clients connect directly to one of the virtual SSL server's IP addresses, configured with the **vips** command. For configuration examples in standalone mode, see the "Stand-alone Web Server Accelerator" chapter in the *Application Guide for SSL Acceleration*. • **off:** When set to off, the VPN Gateway is connected to an Application Switch for SSL offload purposes. The IP address set with the **vips** command corresponds to a virtual IP address on the Application Switch. The default value is **off**.
port <*TCP port number*> Sets the TCP port number to which the virtual SSL server listens. The default is port 443 for all virtual SSL servers. When using the VPN Gateway for SSL Acceleration, the port setting on the VPN Gateway must be accompanied by a redirect filter (on the Application Switch) in which the `dport` value corresponds to the `port` value (on the VPN Gateway).
rip <*real server IP address*> Sets the IP address of the real server to which the virtual SSL server should connect when initiating requests. When using the VPN Gateway in conjunction with an Application Switch, the real server IP address (RIP) should be the set to 0.0.0.0 (the default setting). This setting instructs the VPN Gateway to use the destination IP address found in the received packets, when initiating requests to the virtual server on the Application Switch to which the virtual SSL server has been mapped. When using the VPN Gateway as a stand-alone web server accelerator, without any interoperability with an Application Switch, the real server IP address (RIP) should be set to the IP address of the (single) server that the AVG offloads.

Command Syntax and Usage
If you have enabled the built-in load balancing capabilities of the VPN Gateway, the **rip** command is unavailable. Instead, the IP address for each load balanced real server is specified using the **/cfg/ssl/server #/adv/loadbalanc/backend #/ip** command.
rport <*TCP port number*>
Sets the TCP port to which the virtual SSL server connects. The default `rport` value for all virtual SSL servers that are created is 81. If you are setting up your VPN Gateway as a web server accelerator, the AVG will use this port to send and receive decrypted HTTP information to and from the real web servers. Note that both the virtual server (on the Application Switch) and the real servers must also be configured to listen for AVG traffic on port 81. When using the VPN Gateway as a stand-alone web server accelerator (of a single real web server) in combination with end to end encryption, the rport value should be set to 443. The real web server must also be configured to listen to TCP port 443. If you have enabled the built-in load balancing capabilities of the VPN Gateway, the rport value is neglected. Instead, the TCP port for each load balanced real server is specified using the **/cfg/ssl/server #/adv/loadbalanc/backend #/port** command.
type generic|http|socks
Specifies the virtual SSL server type. Valid options are as follows: • **generic:** When the server type is set to **generic** , the contents is treated as generic data and will not be parsed. • **http:** When the server type is set to **http** , the content is parsed as HTTP requests and responses, and you can use the HTTP configuration options on the non-encrypted contents. For more information about HTTP configuration options. • **socks:** Sets the server type to **SOCKS**. A SOCKS server is only required in configurations supporting the SSL VPN client exclusively, that is, without the need for Portal interaction. To support both the SSL VPN client and the Portal, a portal server is sufficient. A portal server is created automatically when you create a VPN (see /cfg/vpn <id> VPN Menu on page 146). The default SSL server type is set to **generic** .
dnsname
Let you specify fully qualified DNS name of the VIP. **Note:** This menu item is available when SSL server type is set to **http**.
proxy on|off
Specifies whether to use Transparent proxy mode. If **proxy** is set to **on**, the client's real IP address is used when the VPN Gateway forwards client requests

Command Syntax and Usage
to the real servers. Consequently, it is the client's IP address that is logged on the real servers, and not the VPN Gateway's IP address (which is "transparent" to the real servers). To use the Transparent proxy mode, you need to make sure all client traffic is routed back to the clients through the Application Switch. The AVG real server group defined on the Application Switch must use the hash algorithm for server load balancing, and FWLB (Firewall Load Balancing) must be enabled in the appropriate redirect filter on the Application Switch. If **proxy** is set to **off**, the IP address assigned to the VPN Gateway is used when client requests are forwarded to the real servers. If a real web server is logging the client IP address, it will log the AVG's IP address instead of the real client's IP address. When `proxy` is set to **off**, the VPN Gateway works in non-transparent proxy mode, that is. When using non-transparent proxy mode, firewall redirect hash method must not be applied to any real ports on the Application Switch. The default proxy mode value is **on**.
sessionhdr on|off
Sends SSL session information message to the server. The default value is **off**. **Note:** This menu item is available when SSL server type is set to **generic**.
trace
Displays the Trace menu. To view menu options, see/cfg/ssl/server <id> /trace Network Traffic Dump Commands on page 92 .
ssl
Displays the SSL settings menu. For more information, see /cfg/ssl/server <id> /ssl SSL Settings Configuration on page 94.
tcp
Displays the TCP settings menu.
http
Displays the HTTP settings menu. To view menu options, see /cfg/ssl/server <id>/ http HTTP Settings Configuration on page 99. **Note:** This menu item is only available when the SSL server type is set to **http**.
dns
Displays DNS settings menu. For more information about menu options, see /cfg/ssl/server <id>/dns DNS Settings Configuration on page 112.

Command Syntax and Usage
Note: This menu item is available when the SSL server type is set to **socks**.
socks
Displays the Socks settings menu. To view menu options, see /cfg/ssl/server <id> /socks Socks Settings Configuration on page 112. **Note:** This menu item is only available when the SSL server type is set to **socks**.
adv
Displays the Advanced settings menu. To view menu options, see /cfg/ssl/server <id> /adv AdvancedSettings Menu on page 114.
del
Removes the current virtual SSL server.
ena
Enables the current virtual SSL server. This is the default value.
dis
Disables the current virtual SSL server.

/cfg/ssl/server <id> /trace Network Traffic Dump Commands

```
[Trace Menu]
      ssldump    - Create traffic dump
      tcpdump    - Create traffic dump
      ping       - Ping through backend interface
      dnslookup  - Lookup a name in DNS through backend interface
      traceroute - traceroute through backend interface
```

The Trace menu is used for capturing and analyzing SSL and TCP traffic flowing between clients and the selected virtual SSL server on the VPN Gateway. The commands can be useful for debugging purposes. The **ssldump** command will decrypt transmitted data traffic, provided private keys and certificates have been configured properly on the selected virtual SSL server.

The **ssldump** and the **tcpdump** commands can be permanently deactivated in the AVG cluster. For more information, see the **/cfg/sys/distrace** command on page distrace.

Table 21: Trace Menu Options (/cfg/ssl/server/trace)

Command Syntax and Usage
ssldump interactive|tftp|ftp|sftp

Command Syntax and Usage
Creates a dump of the SSL traffic flowing between clients and the currently selected virtual SSL server. The captured information can either be displayed decrypted on screen (the default **interactive** output mode), or saved as a file to a TFTP/FTP/SFTP server. The server can be specified using either the host name or the IP address. If you choose to send the dump as a file to a TFTP server, a number of files will be sent to the server depending on the amount of captured information. A number is appended to the file name given in the CLI, starting at 1 and incremented automatically for additional files. You will be prompted for a destination file name prefix of your own choice. If you choose to send the dump as a file to an FTP server, you will be prompted for the destination file name, as well as a user name and password valid on the specified FTP server. For detailed information about the default flags used when issuing the **ssldump** command, as well as customizing the default filter expression, see the SSLDUMP (1) manual pages under UNIX. For a sample screen output, see CLI Dumps on page 465 ".
tcpdump interactive|tftp|ftp|sftp
Creates a dump of the TCP traffic flowing between clients and the currently selected virtual SSL server. The captured information can either be displayed on screen (the default `interactive` output mode), or saved as a file to a TFTP/FTP/SFTP server. The server can be specified using either the host name or the IP address. You can read a saved TCP traffic dump file using the TCPDUMP or Ethereal application on a remote machine. If you choose to send the dump to a TFTP server, a number of files will be saved on the server depending on the amount of captured information. A number is appended to the file name given in the CLI, starting at 1 and incremented automatically for additional files. You will be prompted for a destination file name prefix of your own choice. If you choose to send the dump as a file to an FTP server, you will be prompted for the destination file name, as well as a user name and password valid on the specified FTP server. For detailed information about the default flags used when issuing the **tcpdump** command, as well as customizing the default filter expression, see the TCPDUMP (8) manual pages under UNIX. For a sample screen output, see CLI Dumps on page 465 ".
ping *<host name or IP address>*
Use this command to verify station-to-station connectivity across the network. If a backend interface is mapped to the current virtual SSL server (only possible for socks servers), the check is made through that backend interface. To map a backend interface to the virtual SSL server, use the **/cfg/ssl/server #/interface** command. To be able to use a host name, the DNS parameters must be configured. To configure a DNS server for the virtual SSL server, use the **/cfg/ssl/server #/dns/servers** command or use the default DNS server (**/cfg/sys/dns**).

Command Syntax and Usage
dnslookup <*host name or IP address*>
Use this command to find the IP address or host name of a machine. If a backend interface is mapped to the current virtual SSL server (only possible for socks servers), the check is made through that backend interface. If a DNS server is configured for the current virtual SSL server, the check is made against that DNS server. To map a backend interface to the virtual SSL server, use the **/cfg/ssl/server #/interface** command. To configure a DNS server for the virtual SSL server, use the **/cfg/ssl /server #/dns/servers** command.
traceroute <*host name or IP address of target station* >
Use this command to identify the route used for station-to-station connectivity across the network. If a backend interface is mapped to the current virtual SSL server (only possible for socks servers), the check is made through that backend interface. To map a backend interface to the virtual SSL server, use the **/cfg/ssl/server #/interface** command. To be able to use a host name, the DNS parameters must be configured. To configure a DNS server for the virtual SSL server, use the **/cfg/ssl/server #/dns/servers** command or use the default DNS server (**/cfg/sys/dns**).

/cfg/ssl/server <id> /ssl SSL Settings Configuration

```
[SSL Settings Menu]
      cert       - Set server certificate
      cachesize  - Set SSL cache size
      cachettl   - Set SSL cache timeout
      cacerts    - Set list of accepted signers of client certificates
      cachain    - Set list of CA chain certificates
      protocol   - Set protocol version
      verify     - Set certificate verification level
      log        - Set syslog detail for ssl connection
      verifylog  - Set syslog detail for client certificate
      ciphers    - Set cipher list
      ena        - Enable SSL
      dis        - Disable SSL
```

The SSL Settings menu is used for configuring SSL-specific settings for a particular virtual SSL server.

Table 22: SSL Settings Menu Options (/cfg/ssl/server/ssl)

Command Syntax and Usage
cert <*certificate index number*>
Specifies which server certificate is used by the current virtual SSL server. To view basic information about available certificates, use the **/info/certs** command. To

Command Syntax and Usage
add a new certificate, see the “Adding Certificates to the AVG” section in the "Certificates and Client Authentication" chapter in the *User's Guide*. Note that each virtual SSL server may only use one server certificate.
cachesize <*number of SSL sessions*>
Sets the size of the SSL cache. The default value is 4000 cached sessions. If you notice that there are many cache misses, the `cachesize` value can be increased for better performance. To view the number of cache misses for a virtual SSL server, use the **/stats/sslstats/server #/cachemisse** command (where you replace " # " with the index number of the desired virtual SSL server).
cachettl <*maximum Time To Live value in seconds*>
Sets the maximum Time To Live (TTL) value for items in the SSL cache, before they are discarded. The default TTL value is 5 minutes.
cacerts <*certificate index number*>
Specifies which of the available CA certificates to use for client authentication. CA certificates are added the same way as an SSL server certificate—either through cut-and-paste, or through TFTP/FTP/SCP/SFTP from a remote host. Both actions are performed from the Certificate menu. To get an overview over available certificates, enter the **/info/certs** command. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified CA certificates, press ENTER when asked to enter the certificate numbers, then answer yes to the question if you want to clear the list. **Note:** If you are using one of the available certificates to generate your own client certificates, you must specify it as a CA certificate to successfully authenticate clients. For more information on client authentication, see the section "Configuring a Virtual SSL Server for Client Authentication" in the "Certificates and Client Authentication" chapter in the *User's Guide*.
cachain <*certificate index number*>
Specifies the CA certificate chain of the server certificate. The chain starts with the issuing CA certificate of the server certificate, and can range up to the root CA certificate. This command explicitly constructs the server certificate chain, which is sent to the browser in addition to the server certificate. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified chain certificates, press ENTER when asked to enter the certificate numbers, then answer yes to the question if you want to clear the list. **Note:** When configuring the virtual SSL server to use chain certificates, the protocol version must be set to SSL3 or SSL23.

Command Syntax and Usage
protocol ssl2|ssl3|ssl23|tls1|tls11|tls12
Specifies the protocol to use when establishing an SSL session with a client. Valid options are as follows: • **ssl2:** Only accept SSL 2.0. • **ssl3:** Only accept SSL 3.0. • **ssl23:** Accept SSL 2.0, SSL 3.0, and TLS 1.0. • **tls1:** Only accept TLS 1.0. • **tls11:** Only accept TLS 1.1. • **tls12:** Only accept TLS 1.2. The default protocol value is **ssl23**. **Note:** Due to an issue with Oracle JRE, to use SSLv3 for AVG Java Applets, users must select the **Use SSL 3.0** check-box only in the **Java Control Panel** (uncheck TLS1.0). JRE does not fallback to lower protocol. AVG Port fowarder and SSH terminal only support SSL 3.0. The Applet will fail to operate if the AVG is configured to use TLS1.0 and above.
verify none|optional|require
Specifies the level of client authentication to use when establishing an SSL session. Valid options are as follows: • None: No client certificate is required. • Optional: A client certificate is requested, but the client need not present one. • Require: The client must present a valid certificate to establish a session. The default verify value is **none**.
log none|accept|reject|both
Syslog message is generated for a successful and failed SSL connection. Valid options are as follows: • None: Syslog message is not generated. • Accept: Generates syslog only for successful SSL connections. • Reject: Generates syslog for unsuccessful SSL connections. • Both: Generates syslog for both successful and unsuccessful SSL connections. The default verify value is **none**.
verifylog
The client certificate events are sent to syslog. Valid options are as follows:

Command Syntax and Usage
• **none:** SSL connection details are not sent to syslog. • **accept:** Sends details of successful SSL connections to syslog. • **reject:** Sends details of unsuccessful SSL connections to syslog. • **both:** Sends details of both, successful and unsuccessful, SSL connections to syslog. The default verify value is **none**.
ciphers <*cipher list*>
Lets you change the default cipher preference list, which corresponds to `ALL:-EXPORT:-LOW!ADH:-SSLv2.` For more information about cipher lists, see the "Cipher List Formats" section in Appendix A, Supported Ciphers, in the *User's Guide*.
ena
Enables SSL on the current virtual SSL server. By default, SSL is enabled on all virtual SSL servers.
dis
Disables SSL on the current virtual SSL server.

/cfg/ssl/server <id> /tcp TCP Settings Configuration

```
[TCP Settings Menu]
      cwrite     - Set client TCP write timeout
      ckeep      - Set client TCP keep alive timeout
      skeep      - Set socks client TCP keep alive heartbeat timeout
      sinterval  - Set socks client TCP keep alive heartbeat interval
      swrite     - Set server TCP write timeout
      sconnect   - Set server TCP connect timeout
      csendbuf   - Set client TCP send buffer size
      crecbuf    - Set client TCP receive buffer size
      ssendbuf   - Set server TCP send buffer size
      srecbuf    - Set server TCP receive buffer size
```

The TCP Settings menu is used for configuring various TCP timeout and buffer size settings on both the client and the virtual SSL server side.

Table 23: TCP Settings Menu Options (/cfg/ssl/server/tcp)

Command Syntax and Usage
cwrite <*client write timeout*>
Sets the timeout value for how long the virtual SSL server should wait for a write operation towards the client(s) to complete. The default client write timeout value is 15m = 15 minutes.

Command Syntax and Usage
ckeep <*client keep alive timeout*>
Sets the timeout value for how long the virtual SSL server should wait before closing an idle session. The default client keep alive timeout value is 15m = 15 minutes.
skeep <*SSL VPN client keep alive timeout*>
If the SSL VPN client stops communicating with the VPN Gateway, this timeout value determines for how long the SSL VPN client should be kept alive before the remote user is logged out. The default SSL VPN client keep alive timeout value is 2m = 2 minutes. The **skeep** command is only available for virtual servers of the socks type.
swrite <*server write timeout*>
Sets the timeout value for how long the virtual SSL server should wait for a write operation towards the backend server(s) to complete. The default server write timeout value is 15m = 15 minutes.
sconnect <*server connect timeout*>
Sets the timeout value for how long the virtual SSL server should wait for a server connection when trying to open a TCP connection. The default server connect timeout value is 30s = 30 seconds.
csendbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the client TCP send buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default client TCP send buffer setting is **auto**.
crecbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the client TCP receive buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default client TCP receive buffer setting is **auto**.
ssendbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the server TCP send buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default server TCP send buffer setting is **auto**.
srecbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the server TCP receive buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default server TCP receive buffer setting is **6000**.

/cfg/ssl/server <id>/http HTTP Settings Configuration

```
[HTTP Settings Menu]
      httpsredir - Set Perform https to http redirect for all traffic
      redirmap   - Redirect mapping
      dynheader  - Dynamically generated headers
      redirect   - Set handle SSL redirect
      downstatus - Set server down reply status
      downurl    - Set Server down redirect URL
      rewrite    - SSL triggered rewrite menu
      securecook - Set add secure option to session cookie
      certcard   - Set enable extra secure smart card setting
      sslheader  - Add SSL header
      sslxheader - Add SSL header with serial in hex
      sslsidhead - Add SSL SID header
      addxfor    - Add X-Forwarded-For header
      addvia     - Add Via header
      addxisd    - Add HTTP-X-ISD debug header
      addfront   - Add Front-End-Https header
      addbeassl  - Add WL-Proxy-SSL header
      addbeacli  - Add WL-Proxy-Client-Cert header
      addclicert - Add Client-Cert as a HTTP header
      addnostore - Add no-cache/no-store HTTP header
      nocachehdr - Remove Cache-Control HTTP header
      compress   - Set compress http data to the client
      cmsie      - Set MSIE session termination bug workaround
      rhost      - Set Rewrite host header to default value
      defaulthos - Set Default host header value
      auth       - User authentication menu
      maxrcount  - Set max number of persistant client requests
      maxline    - Set max line length
      urlobscure - Set URL obfuscation
      sessionhdr - Add X-Nortel-SSL-SessionInfo Header
```

The HTTP Settings menu is used for configuring HTTP-specific settings for a particular virtual SSL server. The HTTP Settings menu is only available if the virtual SSL server has been defined as being of the **`http`** type. For more information about virtual SSL server types, see the **`type`** command on page type generic|http|socks.

Note:

Some of the preceding commands are only available under certain circumstances. If a command is missing in your setup, see the description of the command to find out why it is not currently present.

Table 24: HTTP Settings Menu Options (/cfg/ssl/server/http)

Command Syntax and Usage
`httpsredir on|off` Lets you use a HTTP server to enable HTTP to HTTPS redirection, that is . automatically redirect requests made with HTTP, e.g. http://www.example.com to HTTPS, e.g. https://www.example.com. Note that this is the HTTP server's only purpose.

Command Syntax and Usage
To make this command available, start by creating a virtual SSL server of the HTTP type. Then turn SSL off for the HTTP server. Use the **/cfg/ssl/server #/ssl/dis** command. • **on.** Enables HTTP to HTTPS redirection. Then use the **/cfg/ssl/server #/vips** command to set the virtual IP address of the HTTPS server to which requests should be directed. This is the default value. • **off.** Disables HTTP to HTTPS redirection. The **httpsredir** command is only available when SSL is turned **off**.
redirmap
Displays the Redir Map menu. This command is only available when SSL is turned off and the **httpsredir** command is set to **on**. See the **httpsredir** command.
dynheader
Displays the Dynamic Header menu. To view menu options, see /cfg/ssl/server <id> / http/dynheader Dynamic Header Configuration on page 108.
redirect on|onpath|off|all|allpath

The **redirect** function is designed to enhance a web server's built-in redirect functionality, as illustrated by the example below.
With redirect set to **off**, the client request
`GET /top_page HTTP/1.0`
`Host: www.example.com`
may first be redirected by the web server to
`HTTP/1.0 302 Moved Temporarily`
`Date: Thu, 01 Oct 2005 16:27:51 GMT`
`Server: inets/2.5.3`
`Location: http://www.example.com:81/login`
• With redirect set to **on**, the VPN Gateway rewrites http:// to https:// according to the following pattern:
`HTTP/1.0 302 Moved Temporarily`
`Date: Thu, 01 Oct 2005 16:27:51 GMT`
`Server: inets/2.5.3`
`Location: https://www.example.com/login`
Before rewriting http:// to https://, the VPN Gateway performs a validation of the following criteria:
- The protocol must be HTTP.
- The domain name in the host header of the client request must correspond to the domain name in the Location header of the web server redirect.
- The TCP port in the web server redirect must correspond to the specified **rport** value for the virtual SSL server on the VPN Gateway.

Command Syntax and Usage
Other valid options for the **redirect** command are: • **onpath:** An http:// string that is embedded in the path section of an URL is also rewritten to https://, following the same validation criteria as for the **on** setting. • **off:** No web server redirects are rewritten to https://. • **all:** All web server redirects are rewritten to https://, regardless of the domain name and port in the original client request. Use this setting with caution. • **allpath:** An http:// string that is embedded in the path section of an URL is also rewritten to https://, following the same rules as for the **all** setting. The default **redirect** value is **on**. **Note:** When using the **redirect** feature, the VPN Gateway must be configured to use a DNS server, and the responding DNS server must be able to perform reverse DNS lookups. When the VPN Gateway performs a reverse DNS query of the virtual server IP address (VIP), the resolved name must match the domain name in the Host header of the client request. If the DNS server is unable to perform reverse lookups, the domain name can be configured on the VPN Gateway using the **dnsname** command (see /cfg/ssl/server <id> SSL Server Configuration on page 88).
downstatus unavailable|redirect|reset
Sets the type of behaviour when the HTTP server is down. • **unavailable:** Sends a HTTP 503 "Service Unavailable" message to the client. • **redirect:** Lets you specify a redirect URL using the **downurl** command (see below). • **reset:** Lets the client try to access the server again. The default value is **unavailable**.
downurl <*URL*>
Lets you specify a URL to which the client should be redirected when the HTTP server is down, e.g. http://www.example.com/downinfo.html. This command is only available if the **downstatus** command (see above) is set to **redirect**.
rewrite
Displays the Rewrite menu. To view menu options, see /cfg/ssl/server <id> /http/rewrite HTTP Rewrite Configuration on page 109.
securecook on|off
• **on:** The VPN Gateway sets the Secure attribute on the AVG session cookie and all Set-Cookie headers generated by backend servers. It directs the user agent to use

Command Syntax and Usage
only secure means to contact the origin server whenever it sends back this cookie. For more information, see RFC 2109. • **off:** The Secure attribute is not set. This may cause the AVG session cookie to leak to a trap site through HTTP. This is the default value. The default value is **on**.
certcard
Command used to handle security for client certificates on smart cards. • **on:** Configures the system to log out a remote user from the Portal session as soon as the smart card is removed from the card reader. • **off:** The remote user will still be logged in to the Portal even if the smart card is removed from the card reader. If the user logs out however, the card must be reinserted in the card reader for the user to be able to log back in. The default value is off. **Note:** Turning this feature on will make browser sessions for client certificate users very slow, because a new SSL handshake has to be performed for each GET request and only one HTTP request is allowed per SSL session. The reason is that the client certificate is only sent by the client when a new SSL session is negotiated. To detect that the card has been removed, a new SSL handshake (full handshake, no reuse) must be forced for each request.
sslheader on|off
Specifies how the virtual SSL server handles the optional X-SSL header. When added, the X-SSL header contains information about the particular cipher suite that was used during the SSL session—information that can be logged on the web servers. The information can also be used for web application logical decisions concerning which cipher suites should be accepted. Such a decision would then override the default cipher suite setting for a virtual SSL server on the VPN Gateway. Example of an added X-SSL header: `X-SSL: decrypted=true, ciphers="TLSv1/SSLv3 RC4-MD5"` If you have configured the virtual SSL server to require client certificates, information about the certificate issuer, the certificate subject, and the serial number is extracted from the client certificate and added to the encryption information in the X-SSL header. The length of the Subject (and Issuer) DN is limited to 1000 characters. If it is longer it is truncated. Valid options for the **sslheader** command are: • **on:** An X-SSL header is added to the client request. • **off:** No X-SSL header is added to the client request. The default value is **off**.
sslxheader on|off

Command Syntax and Usage
This command is almost identical to the **sslheader** command (see above), with the difference that the serial number will be in hexadecimal format (with up to 254 hexadecimal digits) instead of decimal format. Usage: If very long serial numbers are used, and/or hexadecimal representation is desired, change the **sslheader** command to off and the **sslxheader** command to on. The default value is **off**.
sslsidhead on|off
If set to **on**, the SSL session ID header is added to the client request. The default value is **off**.
addxfor on|off|anonymous|remove
Specifies how the virtual SSL server handles the optional X-Forwarded-For HTTP header. When added, the X-Forwarded-For header contains information about the peer IP address of the current client connection. This information can be used for enhanced logging purposes. Valid options for the **addxfor** command are: • **on:** An X-Forwarded-For header is added to the current client request. • **off:** No action whatsoever is taken regarding the X-Forwarded-For header. • **anonymous:** The peer IP address of the current client connection is hidden. • **remove:** The X-Forwarded-For header is removed, if present, from the current client request. The default value for the **addxfor** setting is **off**. **Note:** If there are more than one AVG in a cluster and transparent proxy is set to **off**, then firewall load balancing (on the Application Switch) must also be set to **off** for the **addxfor** feature to work.
addvia on|off|anonymous|remove
Specifies how the virtual SSL server handles the through HTTP header. When added, the through HTTP header contains information about the IP address of the virtual server on the Application Switch. Valid options for the **addvia** command are: • **on:** A through header is added to the current client request. • **off:** No action whatsoever is taken regarding the through header. • **anonymous:** The IP address of the virtual server is hidden. • **remove:** The through header is removed, if present, from the current client request. The default value for the **addvia** setting is **on**.

Command Syntax and Usage
addxisd on|off
Specifies how the virtual SSL server handles the optional HTTP-X-ISD header. This header can be used for debugging purposes when end to end encryption or load balancing of backend servers is performed by the VPN Gateway. When added, the extra HTTP-X-ISD header contains information about the IP addresses of both the VPN Gateway that initiated the request and the responding backend server, the internal index number of the responding the backend server, whether connection pooling is enabled, the load balancing type and metric, and finally, whether end to end encryption was performed. Example of an added HTTP-X-ISD header: `HTTP-X-ISD: 192.168.128.25 192.168.100.1 index=2; pool=on; lb=all-roundrobin; type=http-https` Valid options for the **addxisd** command are: • **on:** An HTTP-X-ISD header is added to the client request. • **off:** No HTTP-X-ISD header is added to the client request. The default value for the **addxisd** setting is **off**.
addfront on|off|anonymous|remove
Specifies how the virtual SSL server handles the Front-End-HTTPS header. When using Outlook Web Access (OWA) for Microsoft Exchange in combination with the VPN Gateway, the virtual SSL server must be configured to add this extra header. The Front-End-HTTPS header enables the receiving OWA server to transform embedded HTTP URLs in a correct manner. Valid options for the **addfront** command are: • **on:** An extra Front-End-HTTPS header is added to the client request. • **off:** No extra Front-End-HTTPS header is added to the client request. • **anonymous:** No action whatsoever is taken regarding the Front-End-HTTPS header. • **remove:** The Front-End-HTTPS header is removed, if present, from the current client request. The default value for the **addfront** setting is **off**.
addbeassl on|off|remove
This command is used in SSL Acceleration mode to notify BEA backend servers that an SSL Accelerator is installed in front of the BEA server. The BEA server needs this information to be able to generate functional links. • **on:** Adds the WL-Proxy-SSL: true header to all HTTP requests. • **off:** No WL-Proxy-SSL: true header will be added to HTTP requests • **remove:** The WL-Proxy-SSL: true header is removed (if present), from the current client request. The command is only available for virtual SSL servers of the http type.

Command Syntax and Usage
The default value is **off**.
addbeacli on|off|remove
This command is used in SSL Acceleration mode to append client certificates (if any) to BEA backend servers. • **on:** Adds the WL-Proxy-Client-Cert: <certificate> header to all HTTP requests. • **off:** No WL-Proxy-Client-Cert: <certificate> header will be added to HTTP requests. • **remove:** The WL-Proxy-Client-Cert: <certificate> header is removed (if present), from the current client request. The command is only available for virtual SSL servers of the http type. The default value is **off**.
addclicert on|off
Specifies how the virtual SSL server handles the optional X-Client-Cert HTTP header. When added, the VPN Gateway will insert the entire client certificate (in PEM format) as a multiline HTTP header. The backend web servers can then perform additional user authentication, based on the information in the client certificate. The backend servers can also make use of any auxiliary fields in the client certificate. Valid options for the **addclicert** command are: • **on:** An extra X-Client-Cert HTTP header is added to the client request. • **off:** No extra X-Client-Cert HTTP header is added to the client request. The default value is **off**.
addnostore on|off
Specifies how the virtual SSL server handles the Cache-Control header in a HTTP 1.1 client connection request, or the Pragma header in a HTTP 1.0 client connection request. When added, the inadvertent release or retention of sensitive information is prevented by not allowing any part of the message to be stored in non-volatile storage. Information stored in volatile storage is removed as promptly as possible after having been forwarded. Valid options for the **addnostore** command are: • **on:** A Cache-Control: no-store general-header is added to a client HTTP 1.1 request, and a Pragma: no-cache general-header is added to a client HTTP 1.0 request. • **off:** No Cache-Control or Pragma header is added to the client request. The default value is **on** for all virtual SSL servers of the http and portal types.
nocachehdr on|off
Removes cache-control HTTP header. Valid options are as follows: • **on:** Header is not added to the client request. • **off:** Header is added to the client request.

Command Syntax and Usage
The default value is **off**.
compress on|off
Lets you enable compression of HTTP data to the clients. • **on:** HTTP data is compressed to enable faster transfer to the clients. This may however reduce the encryption throughput on the AVG because the CPU will also be engaged in data compression. • **off:** No compression of HTTP data is performed. The default setting is **off**.
cmsie on|off
Specifies how the virtual SSL server handles the Microsoft Internet Explorer (MSIE) session termination bug workaround. Valid options for the **cmsie** command are: • **on:** The VPN Gateway closes Windows MSIE SSL sessions with a TCP FIN but without an SSL shutdown. This circumvents the MSIE SSL session termination bug. • **off:** The virtual SSL server will always use the FIN (finish) TCP flag to decide when to terminate a client connection. The default value for the **cmsie** setting is **on**.
rhost on|off
Specifies how the virtual SSL server handles the Host header in a HTTP client connection request. The **rhost** setting is mainly used when configuring the VPN Gateway for Global Server Load Balancing in conjunction with the related Application Switch settings. Valid options for the **rhost** command are: • **on:** The Host header in a HTTP client connection request is rewritten to the default value that is defined by using the **/cfg/ssl/server #/http/defaulthos** command. If the client web browser does not include a Host header in its connection request, the default Host header is added. • **off:** No action whatsoever is taken regarding the Host header. The default value for the **rhost** setting is **off**.
defaulthos <*default host header text string*>
Assigns a default text string to the Host header in a HTTP client connection request. The default host header text string you define is applied to the Host header in incoming HTTP client connections requests only when the **rhost** setting is set to **on**.
auth
Displays the WWW-Authenticate Settings menu. To view menu options, see /cfg/ssl/server <id> /http/auth WWW Authentication Configuration on page 111.

Command Syntax and Usage
maxrcount <*numerical value*>
Sets the maximum number of requests for single HTTP/1.1 (or HTTP/1.0 keep-alive) sessions. A HTTP/1.1 session can consist of multiple HTTP requests, one after another. This command lets you set a limit to the number of subsequent requests for a given SSL/TCP session. The default value for the **maxrcount** setting is 40.
maxline <*numerical value*>
Sets the maximum length of HTTP headers in a HTTP client connection request. The default value for the **maxline** setting is 8192.
urlobscure on|off
Displays or hides URL. The default value is **off**.
sessionhdr on|off
Shows the SSL information header. The default value is **off**.

/cfg/ssl/server <id> /http/redirmap Redirect Mapping Configuration

```
[Redir Map Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The Redir Map menu is used to configure HTTP to HTTPS redirect mappings, so that a request for an internal host using HTTP will be redirected to another (or the same) internal host through HTTPS. This is useful for example if your external DNS server resolves a number of internal host names to the same IP address (that is . the server created for HTTP to HTTPS redirect) and you wish to redirect these requests through HTTPS to the intended internal host as configured in your internal DNS server.

To be able to use this feature you should first create an HTTP server for HTTP to HTTPS redirection see the **httpsredir** command.

Table 25: Redirect Mapping Menu Options (/cfg/ssl/server/http/redirmap)

Command Syntax and Usage
list Displays all added entries by index number.
del <*entry by index number*>

Command Syntax and Usage
Removes the specified entry. Use the **list** command to display the index numbers of all entries.
add <*from-host*> <*to-host*>
Adds a host-to-host mapping entry to the current HTTP server. • From-host, e.g. www.example.com. This host name should resolve to the IP address of the HTTP server used for redirection. HTTP requests for this host will be redirected to the to-host (see below). • To-host, e.g. https://www.example2.com/$(path). The **$(path)** variable ensures that any path specified after the host name in the original request will be kept. Advanced example: Configure the external DNS server so that a number of different internal host names resolve to the HTTP server's IP address. To enable automatic redirection of HTTP requests to all these host names, but through a secure portal, enter * (asterisk) as from-host. As to-host, enter e.g. https://portal.example.com/http/$(host)/$(path). The **$(host)** variable ensures that the original host name will be kept. To prevent the unnecessary action of redirecting HTTP requests to the portal through the portal, create an entry (with index number 1) where portal.example.com is the from-host and https://portal.example.com/http /$(path) is the to-host.
insert <*index number to insert at*> <*domain to add*>
Assigns a specific index number to the mapping entry you add. The index number you specify must be in use. Entries with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves a mapping entry up or down in the list of configured entries. The index numbers you specify must be in use. To view all entries currently added to the system configuration, use the **list** command.

/cfg/ssl/server <id> /http/dynheader Dynamic Header Configuration

```
[Dyn Header Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number
```

The Dynamic Header menu is used to create custom HTTP headers to be sent to backend servers. This feature is useful if the backend server requires a specific header. As you configure your custom headers you have the option to specify to which hosts or domains the headers should be sent.

Table 26: Dynamic Header Menu Options (/cfg/ssl/server/http/dynheader)

Command Syntax and Usage
list Displays all headers that are added to the current HTTP server. The headers are listed by their respective index number.
del <*header by index number*>
Removes the specified header. Use the **list** command to display the index numbers of all added entries.
add <*host/domain*> <*header pattern*> Lets you specify a host or domain and the header to send to that host or domain. • Host or domain, e.g. www.example.com or example.com. To add the header for all hosts and domains, enter * (asterisk as host). • Header pattern. Lets you define a custom header to be included in requests to the specified host or to hosts in the specified domain. Header example: **X-cert: client cert <var:clicert> <var:clicert>** will be expanded to a Base 64 encoded version of the client certificate, if one is present. Other available variables are <var:method> (http or https) and <var:sslsid> (SSL session ID in binary format). See Variables on page 28 for an explanation of all variables including instructions on how to use the <md5:string> and <base64:string> variants to compute MD5 checksums and Base 64 encoding of variables.
insert <*index number to insert at*> <*domain to add*> Assigns a specific index number to the header you add. The index number you specify must be in use. Headers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*> Moves a header up or down in the list of configured headers. The index numbers you specify must be in use. To view all headers currently added to the system configuration, use the **list** command.

/cfg/ssl/server <id> /http/rewrite HTTP Rewrite Configuration

```
[Rewrite Menu]
      rewrite     - Set SSL triggered rewrite
      ciphers     - Set accepted ciphers
      response    - Set source of response
      URI         - Set URI with the weak cipher alert
```

The Rewrite menu is used for enabling and configuring the HTTP rewrite functionality for a particular virtual SSL server.

Table 27: Rewrite Menu Options (/cfg/ssl/server/http/rewrite)

Command Syntax and Usage
rewrite on|off Enables or disables the rewrite functionality for the current virtual SSL server. When you enable the rewrite functionality, a customized error message can be sent back to the client's web browser in case the browser is unable to perform the required cipher strength. If the rewrite functionality is not enabled in such a scenario, the client request is simply rejected during the SSL handshake. For more information about how to configure an SSL server to use the rewrite functionality, see the "Configuring the AVG to Rewrite Client Requests" chapter in the *Application Guide for SSL Acceleration*. The default **rewrite** setting is **off**.
ciphers <*cipher list*> Lets you change the cipher list used when the SSL rewrite function is enabled. The default cipher list used when the rewrite function is not enabled corresponds to ALL@STRENGTH . When the rewrite function is enabled, the default rewrite cipher list is **HIGH:MEDIUM** . If you change the default rewrite cipher list from **HIGH:MEDIUM** when having the rewrite function enabled, remember that the rewrite cipher strength must always be higher than the cipher strength specified by using the **/cfg/ssl/server #/ssl/ciphers** command (where the default cipher list is ALL@STRENGTH). For more information about supported ciphers and cipher list formats, see Appendix A, Supported Ciphers, in the *User's Guide*.
response iSD|WebServer Specifies whether the iSD (VPN Gateway) or a web server should handle the response message sent back to the client. When **response** is set to **WebServer** , use the **URI** command to point to a resource on a web server that can provide a customized error message. The default **response** setting is **iSD**.
URI <*IP address and path to web server resource for response message*> Sets the URI pointing to a resource on a WebServer that provides the response message (when **response** is set to **WebServer**).

/cfg/ssl/server <id> /http/auth WWW Authentication Configuration

```
[WWW-Authenticate Settings Menu]
      mode       - Set authentication mode
      realm      - Set realm for authentication
      vpn        - Set vpn
      ena        - Enable HTTP User Authentication
      dis        - Disable HTTP User Authentication
```

The WWW-Authenticate Settings menu is used for restricting access to internal web servers whose DNS names corresponds to the virtual server IP (VIP) address assigned to the current SSL server.

Users who try to access the resources included in the WWW authentication scheme need to provide their user name and password. These credentials are then validated against one or more authentication methods and user access groups defined in the VPN that you specify as part of the WWW authentication configuration. In the context of WWW authentication, the significance of the VPN is limited to the authentication method used for validating a user's credentials, as well as the validation of a user's group membership and associated access rules.

The WWW-Authenticate Settings menu is only available if the virtual SSL server has been defined as being of the **http** type. For more information about virtual SSL server types, see the **type** command on type generic|http|socks.

Table 28: WWW-Authenticate Settings Menu Options (/cfg/ssl/server/http/auth)

Command Syntax and Usage
mode basic|digest|portal Sets the authentication mode used by the virtual SSL server. Valid options are as follows: • **basic:** Displays a login popup window when the user tries to access the restricted resource. Use basic mode if you do not have a Portal through which users can be authenticated. • **digest:** Not implemented yet. • **portal:** Displays the Portal login page when the user tries to access the restricted resource. Remote users who are already logged in to the Portal when trying to access a resource restricted by WWW authentication does not have to log in again. The default authentication mode is **basic**.
realm <*name of the realm*> Assigns a name to the realm. The realm is mainly for the user's own information, and is displayed in the login popup window (when using basic authentication mode). The default realm name is **Xnet**.

Command Syntax and Usage
vpn <*VPN number*>
Sets the VPN, identified by its domain number. In the context of WWW authentication, the significance of the VPN is limited to applying the authentication methods in the VPN configuration. For basic authentication mode, specify the VPN in which you have defined the user access groups that should be provided access to the restricted resource. Make sure that the access rules allow access to the password restricted resource. For portal authentication mode, specify the VPN whose web Portal you want to use for authenticating users who try to access the password restricted resource. As when using basic authentication mode, the VPN you specify must encompass the user access groups that should be provided access to the restricted resource.
ena
Enables HTTP user authentication.
dis
Disables HTTP user authentication.

/cfg/ssl/server <id>/dns DNS Settings Configuration

```
[DNS Settings Menu]
      search     - Set DNS search list
```

You can use the DNS Settings Menu to search the Domain Name Servers.

Table 29: DNS Settings Menu Options (/cfg/ssl/server/dns)

Command Syntax and Usage
search
Lets you search the Domain Name Servers. To search, enter the DNS values separated by comma.

/cfg/ssl/server <id> /socks Socks Settings Configuration

```
[Socks Settings Menu]
      version    - Set socks version
      methods    - Set socks methods
      commands   - Set socks commands
      vpn        - Set vpn
      defgroup   - Set default group
```

From VPN Gateway version 4.1, SOCKS support is also enabled for portal servers. The Socks Settings menu is still available for backward compatibility and for customers who wants support for the SSL VPN client only (that is . when no Portal is required).

The Socks Settings menu is only available if the virtual SSL server has been defined as being of the `socks` type. For more information about virtual SSL server types, see the **`type`** command.

Table 30: Socks Settings Menu Options (/cfg/ssl/server/socks)

Command Syntax and Usage
`version v4|v5|v45` Sets the Socks protocol version used in the communication between the AVG cluster and SSL VPN socks clients. Valid options are as follows: • **`v4:`** Only protocol version 4 is accepted. • **`v5:`** Only protocol version 5 is accepted, and socks clients using version 4 are rejected. • **`v45:`** Both protocol versions 4 and 5 are accepted, and socks clients using either version are accepted. The default Socks protocol setting is v45. **Note:** Socks version 4 neither supports strong authentication, nor authentication method negotiation.
`methods user|none` Sets the preferred Socks authentication method(s) for Socks protocol version 5. For clients connecting with Socks protocol version 4, these settings are ignored because version 4 does not support authentication. The authentication method you set here comes into play when a remote user connects to the VPN using the SSL VPN client (that is . not through the Portal). The available options are: • **`user:`** Username/Password client authentication is required. • **`none:`** No client authentication is required. When setting the Socks authentication method to **`none`**, make sure you also specify a default user access group (using the **`defgroup`** command). The default Socks authentication method is set to **`user`**. **Note:** The Socks authentication method you specify here interacts with the authentication methods defined in the VPN using the **`/cfg/vpn <id>/aaa/auth`** command. When the Socks method is set to **`user`**, a remote user connecting to the VPN through the SSL VPN client is prompted for the user name and password through a pop-up window. These credentials are then verified against one of the authentication methods defined in the VPN. If a match is found, the user is authenticated and the user's group membership is determined.
`commands` <*connect, bind*>

Command Syntax and Usage
Sets the permitted Socks client command(s). If you enter more than one command, separate the entries using comma (,). The available options are: • **connect:** Allows the Socks client to send a CONNECT request to the server when it wants to establish a connection to an application server (the destination host). • **bind:** Allows the Socks client to send a BIND request when it wants to prepare for an inbound connection from an application server (the destination host). A client BIND request is only sent after a primary connection to the application server has been established with a CONNECT request. The default Socks commands are set to **connect** and **bind**.
vpn <VPN identified by number)
Maps the current socks server to a configured VPN. To view available VPNs, type **/cfg/vpn** and press TAB.
defgroup <*default group by name*>
Sets an existing user access group that has been defined using the **/cfg/vpn <id>/aaa/group** command as the default user access group. The default group is applied when an SSL VPN user's group membership cannot be determined. This typically happens when an SSL VPN user connects to the VPN in "transparent mode", and the Socks authentication is set to **none** . In such a case, the non-authenticated SSL VPN user will automatically become a member of the specified default group, and the access control lists associated with the default group will determine which rights are granted to the user. **Note:** Because the user to which the default group applies is not authenticated by any means, make sure that the access control lists associated with the group do not grant excessive rights.

/cfg/ssl/server <id> /adv AdvancedSettings Menu

```
[Advanced Settings Menu]
      string     - String menu
      blockstrin - Set strings to block
      pool       - Connection pooling menu
      traflog    - UDP syslog Traffic Log menu
      loadbalanc - Load balancing menu
      sslconnect - SSL connect menu
```

The Advanced Settings menu is used for handling the connection pooling, load balancing, and end to end encryption capabilities of the selected virtual SSL server. The number of menu items available in the Advanced Settings menu vary according to the type of virtual SSL server currently selected.

Table 31: Advanced Settings Menu Options (/cfg/ssl/server/adv)

Command Syntax and Usage
string Displays the Load Balancing String menu. To view menu options, see /cfg/ssl/server <id> /adv /string <load balancing string id> Load Balancing Strings Configuration on page 116. **Note:** The string menu item is only available when the virtual SSL server type is set to the generic or http type.
blockstrin <*string numbers*> Specifies which of the defined match strings that are used for blocking client requests. If a client request contains data that matches one of the specified string definitions, the client connection request is terminated. To clear all currently specified blocking strings, press ENTER when asked to enter string numbers, then answer yes to the question if you want to clear the list. **Note:** The blockstrin command is only available when the virtual SSL server type is set to the generic or http type.
pool Displays the Pool Settings menu. To view menu options, see /cfg/ssl/server <id> /adv/pool Connection Pooling Configuration on page 118. **Note:** The pool menu item is only available when the virtual SSL server type is set to http.
traflog Displays the Traffic Log Settings menu. To view menu options, see /cfg/ssl/server <id>/adv/traflog Traffic Syslog Configuration on page 119. **Note:** The traflog menu item is only available when the virtual SSL server type is set to http or portal.
loadbalanc Displays the Load Balancing Settings menu. To view menu options, see /cfg/ssl/server <id> /adv /loadbalanc Load Balancing Settings on page 121. **Note:** The loadbalanc menu item is only available when the virtual SSL server is set to the **generic** or **http** type.
sslconnect

Command Syntax and Usage
Displays the SSL Connect Settings menu. To view menu options, see /cfg/ssl/server <number> /adv /sslconnect SSL Connect Configuration on page 134. **Note:** The sslconnect menu item is only available when the virtual SSL server is set to one of the following: **generic**, **http,** or **portal**.

/cfg/ssl/server <id> /adv /string <load balancing string id> Load Balancing Strings Configuration

```
[LB String 1 Menu]
      match      - Set string to match
      location   - Set locations to perform the match in
      icase      - Set ignore case in to match
      negate     - Set negate the result of the match
      del        - Remove string
```

The LB String menu is used for defining strings matching the specified location in a client request. Resulting matches can then be taken into account in the load balancing configuration of the backend servers. When a backend server is configured to use `string` as the load balancing type, the backend server is only load balanced if a match of the defined string and location is found in a client request. To access the LB String menu, the selected virtual SSL server must be set to the generic or http type.

Table 32: LB String Menu Options (/cfg/ssl/server/adv/string)

Command Syntax and Usage
match Lets you define the string matched against incoming client requests handled by the virtual SSL server. A match string may contain the asterisk (*) wildcard character to represent one or more unspecified characters. Example: ***.gif** **Note:** After having defined a match string, you must also specify the desired match location(s).
location <*macro, method, or header*>
Specifies the client request location(s) to which the match string is mapped. A match only occurs when the match string is found in the specified location. Valid match locations can be the name of a header in an HTTP request (such as User-Agent), or an HTTP method (such as GET). • Valid match locations are the following special components that may appear in a URL: - **Params** (object parameters)

Command Syntax and Usage

- **Query** (query information)

If used, these components appear in the URL in accordance with this generic syntax:
<*scheme*> **:// <net_loc> /** <*path*> **;** <*params*> **?** <*query*> **#** <*fragment*>

- A valid special string location is:
  - **cookie-override:** By default, cookie-based persistence overrides string load balancing settings. To override persistence for a string, add **cookie-override** to the location value for the string. In this way, it is possible to use cookie-based persistence for for example all URLs except those ending with *.gif. For a match to occur, you must also specify a valid match location, e.g. **URL, cookie-override**.
- The valid macro location values are:
  - **url:** all of the valid method fields are searched for a match of the defined string. A match of the defined string will only occur if the match string is found in one of the known methods listed below.
  - **unknown:** unknown method for the VPN Gateway. A match will only occur if a method other than the known methods is found. (If you specify **url,unknown,** as the locations, a match will occur if the match string is found in either a known or unknown method, or both.)
  - **header:** all of the valid header fields are searched for a match of the defined string. A match will only occur if the match string is found in one of the known headers.
  - **other:** unknown header field for the VPN Gateway. A match will only occur if a header other than the known headers is found. (If you specify **header,other,** as the locations, a match will occur if the match string is found in either a known or unknown header, or both.)
- Valid methods are: **options, get, head, post, put, delete, trace,** and **connect**.
- Valid headers are: **accept, accept-charset, accept-encoding, accept- language, accept-ranges, age, allow, authorization, cache-control, connection, content-base, content-encoding, content-uage, content-length, content-location, content-md5, content-range, content-type, cookie, cookie2, date, etag, expires, fragment, from, host, if-match, if-modified-since, if-none-match, if-range, if-unmodified-since, keep-alive, last-modified, location, max-forwards, params, pragma, pragma, proxy-authenticate, proxy-authorization, proxy- connection, public, query, range, referer, retry-after, server, set-cookie, set-cookie, transfer-encoding, upgrade, user-agent, vary,**

Command Syntax and Usage
through, warning, www-authenticate, x-forwarded-for, and **x-ssl**.
To enter multiple locations, separate the location names with comma (,). To look for a match string in all components of a URL, specify the following as the location: **URL,Params,Query**.
icase on|off
Specifies whether case should be considered when searching for a match of the defined string in the specified location of a client request. When set to **off**, a match string defined as ***.GIF** is considered different data than the ***.gif** string found in the URI of a client request, and a match will therefore not occur. The default **icase** setting is **on**, which means that case is ignored.
negate on|off
Specifies whether the match string you have defined should be negated when searching for a match in a client request. When set to **on** , all client requests that do not contain the defined match string in the specified location will induce a match. The default negate setting is **off**.
del
Removes the current match string.

/cfg/ssl/server <id> /adv/pool Connection Pooling Configuration

```
[Pool Settings Menu]
      timeout    - Set pool age timeout
      ena        - Enable connection pooling
      dis        - Disable connection pooling
```

The Pool Settings menu is used for configuring the connection pooling settings of the VPN Gateway. Connection pooling provides for the reuse of SSL sessions to improve throughput. When the VPN Gateway load balances the backend servers, it can pool both encrypted (port 443) and unencrypted (port 81) server side connections. To access the Pool Settings menu, the selected virtual SSL server must be set to the http type.

Table 33: Pool Settings Menu Options (/cfg/ssl/server/adv/pool)

Command Syntax and Usage
timeout *<timeout value in seconds>*
Sets the time frame during which a client connection can be idle before the client socket is closed. The default value is 15 seconds.
ena

Command Syntax and Usage
Enables pooling of server side connections for the selected virtual SSL server. **Note:** When connection pooling is enabled, transparent proxy mode must be set to **off**. Transparent proxy mode is configured by using the **/cfg/ssl/server #/proxy** command. The default proxy mode value is **on**.
dis
Disables pooling of server side sockets for the selected virtual SSL server.

/cfg/ssl/server <id>/adv/traflog Traffic Syslog Configuration

```
[Traffic Log Settings Menu]
      protocol   - Set syslog protocol
      sysloghost - Set syslog host IP
      udpport    - Set syslog portnumber
      priority   - Set syslog priority
      facility   - Set syslog facility
      ena        - Enable traffic UDP syslog logging
      dis        - Disable traffic UDP syslog logging
```

The Traffic Log Settings menu is used for configuring a syslog server, to which UDP syslog messages for all HTTP requests handled by the currently selected virtual SSL server, can be sent. Enabling traffic logging through syslog messages will generate a substantial amount of network traffic, and also place additional CPU load on each AVG device in the cluster. Besides, syslog servers are not generally intended for this type of log messages, and the syslog server might therefore not be able to cope with the amount of syslog messages generated within a cluster of multiple AVG devices. In environments where traffic logging must be performed on the SSL terminating device itself due to laws or regulations, traffic logging through syslog messages can be used. It can also be used temporarily for debugging purposes. This setting will generate traffic; therefore it is recommended that you set up syslog on the backend server if possible.

In general, it is therefore recommended that traffic logging is performed on the backend web servers instead. The traffic logging performed by backend web servers can be enhanced by configuring the VPN Gateway to add certain HTTP headers. For more information about available extra HTTP headers, see the HTTP Settings menu on /cfg/vpn <id> /server/http HTTP Settings Configuration on page 258.

Below is an example of a syslog message generated on an AVG device: `Mar 8 14:14:33 192.168.128.24 <ISD-SSL>: 192.168.128.189 TLSv1/SSLv3 DES-CBC3-SHA "GET / HTTP/1.0"`

To access the Traffic Log Settings menu, the selected virtual SSL server must be set to either the http type or the portal type.

Table 34: Traffic Log Settings Menu Options (/cfg/ssl/server/adv/traflog)

Command Syntax and Usage
protocol bsd|ietf Specifies the syslog message format. Valid options for **protocol** command are: • **bsd**: Syslog message appears in bsd format. The IP and facility information must be provided. To configure facility, see facility. • **ietf**: Syslog message appears in ietf format. The IP and facility information is not required. The default message format is **bsd**.
sysloghost <*IP address of syslog server*> Specifies the IP address of the syslog server to which syslog messages will be sent using a UDP (User Datagram Protocol) connection.
udpport <*UDP port number of syslog server*> Specifies the UDP port number of the syslog server. The default UDP syslog server port number is set to 514.
priority debug|info|notice Configures the priority level of syslog messages that are sent. Valid priority levels, listed from low to high, are: • **debug:** Messages that contain information mainly of use only for debugging purposes. • **info:** Informational messages. • **notice:** Conditions that are not error conditions, but should possibly be handled specially. The default priority level is set to **info**.
facility auth|authpriv|daemon|local0-7 Configures the facility parameter of syslog messages. The facility parameter is used to specify what type of program is logging the message. This lets the configuration file specify that messages from different facilities will be handled differently. The default facility parameter is set to **local4**.
ena Enables traffic logging through syslog messages to the specified syslog server.
dis Disables traffic logging through syslog messages to the specified syslog server. Traffic logging through syslog messages is disabled by default.

/cfg/ssl/server <id> /adv /loadbalanc Load Balancing Settings

```
[Load Balancing Settings Menu]
      type       - Set load balancing type
      persistenc - Set persistence strategy
      cookie     - Cookie settings menu
      metric     - Set load balancing metric
      health     - Set health check type
      script     - Health check script menu
      interval   - Set health check interval (s)
      remotessl  - Remote SSL connect menu
      grace      - Set graceful shutdown mode
      backend    - Backend servers menu
      ena        - Enable load balancing
      dis        - Disable load balancing
```

The Load Balancing Settings menu is used for configuring the various settings related to persistency in client connections, load balancing of backend servers, and health checking of the backend servers. To access the Load Balancing Settings menu, the selected virtual SSL server must be set to the generic or http type.

Table 35: Load Balancing Settings Menu Options (/cfg/ssl/server/adv /loadbalanc)

Command Syntax and Usage
type all|string Specifies the load balancing type applied to configured backend servers. Valid options are as follows: • **all:** All backend servers are load balanced according to the specified load balancing metric. Load balancing strings that may have been defined are ignored. • **string:** Only those backend servers for which you have configured one or more match strings are load balanced. Load balancing of these backend servers occur only when a match of the specified string is found in a client request; the load balancing is then performed in accordance with the load balancing metric you have specified. To load balance all backend servers when **type** is set to **string**, make sure you have configured each backend server to use one or more match strings. Backend servers are configured by using the **/cfg/ssl/server #/adv/loadbalanc/backend #** command. **Note:** When the load balancing type is set to **string** , persistency options set to **cookie** or **session** are ignored.
persistenc none|cookie|session Specifies the method to use to obtain persistency in client connections. When a client initiates a connection request to establish a new session, the connection is issued to a backend server according to the load balancing metric you have specified. For all subsequent client requests within an established session,

Command Syntax and Usage
however, the chosen persistency method comes into play and overrides the load balancing metric. Valid options for obtaining persistency in client connections are: • **none:** Specifies that no method is used to obtain persistency in client connections. • **cookie:** Specifies that persistency in client connections is based on cookie information generated and inserted by the VPN Gateway. To successfully use this option, client browsers must accept cookies. • **session:** Specifies that persistency in client connections is based on the SSL session information. The default persistence method is **none**. Note that the **cookie** and **session** persistency options are ignored when the load balancing **type** is set to **string**. For more information on the **type** command, see type all|string.
cookie
Displays the Cookie Settings menu. To view menu options, see /cfg/ssl/server <id> /adv/loadbalanc /cookie Cookie Settings Configuration on page 124.
metric hash|roundrobin|leastconn
Specifies the load balancing metric to use for determining which of the configured backend servers that will be the target of the next client request. Valid options are as follows: • **hash:** With this option, a hash metric on the source IP address information in a client connection request is used to select a backend server. • **roundrobin:** Round robin. With this option, new client connection requests are issued to each backend server in turn in a continuously repeating sequence. • **leastconn:** Least connections. With this option, a new client connection request is issued to the backend server with the fewest current connections. The number of connections currently open on each backend server is measured in real time. The **leastconn** option is the most self-regulating, with the fastest servers typically getting the most connections over time, due to their ability to accept, process, and shut down connections faster than slower servers. The default load balancing metric is **hash**.
health none|tcp|ssl|auto|script
Specifies the health check method the selected virtual SSL server should use when health checking the backend servers. Valid options are as follows: • **none:** No health checking of backend servers. If load balancing is enabled, all backend servers are included in the load balancing scheme and the backend servers will at all times be considered as "up". Failed connections to backend

Command Syntax and Usage
servers are still logged (as a total) and can be viewed using the **/stats/sslstats/server #/becnctfail** command. • **tcp:** A TCP connection is opened to the backend servers, and is then closed. • **ssl:** A TCP connection is opened to the backend servers, and an SSL connection is then established. Thereafter, the SSL connection is shut down and the TCP connection is closed. Using the ssl health check method requires that you have enabled SSL connect for the current virtual SSL server. To view the current SSL connect settings, enter the following command: **/cfg/ssl/server #/adv/sslconnect/cur** • **auto:** The default health check method, which uses a built-in script. For more information about the built-in scripts, see the "Script-Based Health Checks" chapter in the *Application Guide for SSL Acceleration*. • **script:** Uses a customized health check script, which must first be created by using commands available in the Health Check Script menu. For more information about creating customized health check scripts, see the "Script-Based Health Checks" chapter in the *Application Guide for SSL Acceleration*. The default health check method is **auto**.
script
Displays the Health Check Script menu. To view menu options, see /cfg/ssl/server <id> /adv/loadbalanc /script Health Check Script Configuration on page 127.
interval <*health check interval in seconds*>
Sets the interval in seconds for health checks of the backend servers to occur. The default health check interval is 10 seconds. **Note:** Each VPN Gateway in the cluster performs its own health checking of backend servers. Therefore, if you set the health check interval to a low value, a considerable amount of network traffic may be generated. The amount of network traffic increases with the number of AVGs in the cluster and the number of backend servers included in the health checking.
remotessl
Displays the Remote SSL Connect Settings menu. To view menu options, see /cfg/ssl/server <id> /adv/loadbalanc /remotessl Remote SSL Connect Configuration on page 129.
grace
on- Enables the graceful shutdown menu. When the graceful shutdown option is enabled, all the incoming new connections are blocked and existing connections within the AVG continue to process. off- Disbales the graceful shutdown menu. When the graceful shutdown option is enabled, all the incoming new connections are allowed and existing connections within the AVG stops.

Command Syntax and Usage
backend
Displays the Backend Server menu. To view menu options, see /cfg/ssl/server <id> /adv/loadbalanc /backend <server id> Backend Server Configuration on page 130.
ena
Enables load balancing of backend servers.
dis
Disables load balancing of backend servers.

/cfg/ssl/server <id> /adv/loadbalanc /cookie Cookie Settings Configuration

```
[Cookie Settings Menu]
      mode       - Set cookie mode
      name       - Set cookie name
      domain     - Set cookie domain
      expires    - Set cookie expires
      expiresdel - Set cookie expires delta
      localvips  - Configure other local VIPs
      offset     - Set cookie value offset
      length     - Set cookie value length
```

The Cookie Settings menu is used for configuring the cookie properties used by the selected virtual SSL server when **cookie** is the selected persistence strategy. The Cookie Settings menu is only available when you have configured the virtual SSL server to use cookie-based persistency. For more information on persistency options, see the **persistenc** commandon persistenc none|cookie|session.

Table 36: Cookie Settings Menu Options (/cfg/ssl/server/adv/loadbalanc/cookie)

Command Syntax and Usage
mode insert|passive|rewrite
Specifies the mode for cookie-based persistence. The default cookie mode is **insert (i)**. The following three modes are available: • **insert (i)**: Insert mode. When a client sends a connection request without a cookie, the backend server responds with the requested data, and the VPN Gateway inserts a cookie into the data packet. The VPN Gateway then uses this cookie on all subsequent connection requests (within a given session) from the same client to bind to the backend server that was first selected using the current load balancing metric. • **passive (p):** Passive mode. When selecting this mode, the backend server must be configured to embed a cookie in the response to the client request. The

Command Syntax and Usage

backend server may be configured to embed a cookie that contains either a backend server IP address in hexadecimal form, or a string of characters as the cookie value. The VPN Gateway will then look for this cookie in all subsequent connection requests (within a given session) from the same client, before establishing a connection to a backend server.

- If the backend server embeds its own IP address in the cookie, the VPN Gateway will use the IP address information in the cookie to direct all subsequent traffic within a given session to the corresponding backend server.
- If the backend server embeds a string of characters as the cookie value, the VPN Gateway will perform a hash on the cookie value. The VPN Gateway will then select a backend server and direct all subsequent traffic within a given session to the same backend server, based on the hashed cookie value.

- **rewrite (r)**: Rewrite mode. When selecting this mode, the backend server must be configured to return a special persistence cookie, which the VPN Gateway is configured to recognize. When recognized, the VPN Gateway intercepts the cookie and rewrites the value to include server-specific information before sending it on to the client. Subsequent connection requests (within a given session) from the same client are sent to the same backend server.

For configuration examples including the three different cookie-based persistence modes, see the section "Configuring Cookie-Based Persistence" in the "Load Balancing of Backend Servers" chapter of the *Application Guide for SSL Acceleration*.

name <*cookie name*>

Sets a cookie name that can be used to identify the cookie used by the virtual SSL server.
The default cookie name is **ISDSSL**.

domain <*cookie domain name*>

Sets a domain name that is valid for the cookie, e.g. .example.com. In global server load balancing (GSLB) configurations, the case might be that the client browser returns the cookie to another server than the server from which it was originally sent, if they both respond to the same host name (e.g. www.example.com). Since this other server will not recognize the cookie id, it will forward the cookie to other servers using the domain name specified as cookie domain name.
Only used for Insert mode.

expires <*date and time*>

Sets an absolute expiration date for the cookie. The cookie will be cached on the client's local disk until the date expires, then it will be deleted automatically.
Enter the date according to one of the following formats:

```
Sun, 06 Nov 2005 08:49:37 GMT
Sunday, 06-Nov-04 08:49:37 GMT
Sun Nov 6 08:49:37 2005
```

Command Syntax and Usage
If no expiration date is set, the cookie will expire as soon as the client web browser is shut down. Only used for Insert mode.
expiresdel <*value in seconds*>
Sets the time frame during which the cookie will be active. When this time has expired, the cookie will be deleted automatically. If you want to specify a value in hours, enter an integer directly followed by the letter **h** . If you want to specify a value in minutes, enter an integer directly followed by the letter **m** . If you enter an integer only, the value in seconds is implied. To specify a value consisting of hours, minutes and seconds, enter e.g. **12h15m30s**. If no expiration value is set, the cookie will expire as soon as the client web browser is shut down. Only used for Insert mode.
localvips
Configures other local virtual server IP addresses. The local server needs to recognize sessions that belong to the official site virtual server IP address, as well as its own virtual server IP address that is used in a global server load balancing (GSLB) configuration.
offset <*cookie offset value in bytes (1-64)*>
Sets the starting point of the real cookie value within a longer string. The offset value directs the VPN Gateway to start looking for the real cookie value at the specified location in the string. The default cookie offset value is **1** (byte).
length <*cookie length value in bytes (0-64)*>
Sets the number of bytes to extract for the cookie value within a longer string. • For Passive cookie mode, if you have configured your backend server to use a string of characters that is embedded as the cookie value, you can set the length can be set from 0 to 64 bytes. • For Insert or Rewrite cookie mode, if you want the VPN Gateway to include the IP address of the backend server in the cookie value, you must set the cookie length to 8. The cookie mode can be set to **insert**, **rewrite**, or **passive**. • For Insert or Rewrite cookie mode, if you want the VPN Gateway to include both the IP address of the backend server and the IP address of the virtual server (the VIP on the Application Switch) in the cookie value, you must set the cookie length to 16. The default cookie length value is 8 .

/cfg/ssl/server <id> /adv/loadbalanc /script Health Check Script Configuration

```
[Health Check Script Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The Health Check Script menu is used for creating a customized script used for health checking backend servers that are load balanced by the VPN Gateway. The script you create is only applied when you have specified script as the health check method in the menu for /cfg/ssl/server <id> /adv /loadbalanc Load Balancing Settings on page 121 (**/cfg/ssl/server #/adv/loadbalanc/health**). For detailed information about creating customized health check scripts, see the chapter "ScriptBased Health Checks" in the *Application Guide for SSL Acceleration*.

Table 37: Health Check Script Menu Options (/cfg/ssl/server/adv/loadbalanc /script)

Command Syntax and Usage
list Lists the current health check script, where each line is a script command and represented by a unique index number. The lines in the script are processed one after the other, starting from the lowest index number and ending with the highest index number.
del *<index number>* Removes the line in the health check script represented by the index number you specify. Use the **list** command to view all lines and related index numbers in the current health check script.
add *<script command> <timeout in seconds> <argument>* Lets you create a customized health check script, line by line, or add a script command to an existing health check script. Each added script line is automatically assigned the next available index number. A customized health check script is only applied when you have selected **script** as the health check type. The following script commands are available: • **auto_open**: Opens a TCP connection to the backend servers. For those backend servers on which SSL connect is enabled, the command also opens a SSL connection. • **auto_close**: Closes the TCP connection that was opened using the **auto_open** command. In case the **auto_open** command also established an SSL connection, the SSL connection is shut down prior to closing the TCP connection.

Command Syntax and Usage
• **open**: Opens a TCP connection to the specified IP address or backend servers. • **close**: Closes the TCP connection that was opened using the **open** script command. • **ssl_open**: Opens a SSL connection to the specified IP address or backend servers. The **ssl_open** script command must always be preceded by the regular **open** command. Using the **ssl_open** command also requires that SSL connect is enabled. You can view the current SSL settings by using the **/cfg/ssl/server #/adv/sslconnect/cur** command. • **ssl_close**: Closes the SSL connection that was opened using the **ssl_open** command. The **ssl_close** script command must always be followed by the regular **close** command. • **send**: Sends for example a **GET** request you specify as an argument to the **send** command, such as "**GET /index.html HTTP/1.0 \r\n\r\n**" to the backend servers. • **expect**: Specifies the string that is required in the response from the backend servers, in reaction to the **send** argument you specified. An example of an **expect** argument used with the **send** argument above could be "**^HTTP/1\.[1,0] +200**". The **expect** arguments are based on the usage of extended POSIX regular expressions. The arguments you can define vary depending on the script command: • When using the **auto_open, open,** or the **ssl_open** script commands, IP address and TCP port is a valid argument. Example: 192.168.128.88:110 If you don't specify an IP address and TCP port as an argument for these script commands, the IP addresses of the load balanced backend servers are implicit. • When using the **auto_close, close,** or the **ssl_close** script commands, you don't need to repeat the IP address and TCP port given as an argument for the **auto_open, open,** or **ssl_open** script commands since the same argument is implicit. • When using the **send** script command, a typical HTTP request message can be defined as an argument. Example: "**GET /index.html HTTP/1.0 \r\n\r\n**" • When using the **expect** script command, you can define arguments based on extended POSIX regular expressions. The data received in response to the **send** command is matched against the string you have defined in the argument for the **expect** command. If a match is found, the script command is considered successful.
insert *<index number> <script command> <timeout in seconds> <argument>*
Lets you assign a specific index number to the script line you add. The index number you specify must be in use. Script lines with an index number higher than

Command Syntax and Usage
(and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Lets you move a script line up or down in the health check script. The script commands are processed one after the other, starting from the lowest index number and ending with the highest index number. To view all lines and script commands in the script, use the **list** command.

/cfg/ssl/server <id> /adv/loadbalanc /remotessl Remote SSL Connect Configuration

```
[Remote SSL Connect Settings Menu]
      protocol   - Set protocol version
      cert       - Set client certificate
      ciphers    - Set accepted ciphers for ssl connect
      verify     - Verify server menu
```

The Remote SSL Connect Settings menu is used for configuring the SSL protocol, the preferred cipher list, and client authentication for SSL connections between the VPN Gateway(s) and the backend servers.

Table 38: Remote SSL Connect Settings Menu Options (/cfg/ssl/server/adv/loadbalanc/remotessl)

Command Syntax and Usage
protocol ssl2|ssl3|ssl23|tls1|tls11|tls12
Specifies the protocol the virtual SSL server should propose when establishing an SSL session with an SSL-enabled backend server. Valid options are as follows: • **ssl2**: Propose using only SSL 2.0. • **ssl3**: Propose using only SSL 3.0. • **ssl23**: Propose using any of SSL 2.0, SSL 3.0, or TLS 1.0. • **tls1**: Propose using only TLS 1.0. • **tls11**: Propose using only TLS 1.1. • **tls12**: Propose using only TLS 1.2. The default protocol value is **ssl23**.
cert <*client certificate by index number*>
Specifies which client certificate the selected virtual SSL server should present to the backend servers, in case the SSL software on the backend servers is configured to require a client certificate. Client authentication is typically very

Command Syntax and Usage
seldom used for SSL connections between the VPN Gateways and the backend servers, as the client is known in these circumstances. To view basic information about available certificates, use the **/info/certs** command. To generate a client certificate, see the "Generating Client Certificates" section in the "Certificates and Client Authentication" chapter in the *User's Guide*.
ciphers <*cipher list format*>
Specifies the list of preferred ciphers. This information is sent to the backend servers during the SSL handshake. The default cipher list corresponds to `ALL:-EXPORT:-LOW!ADH:-SSLv2` , which should be appropriate in most cases. The default cipher list provides for using lighter encryption algorithms between the VPN Gateways and the backend servers than what is normally used between Internet clients and the VPN Gateways. This is desirable mainly in terms of SSL performance. Since both the VPN Gateways and the backend servers typically are behind a firewall in physically secured premises, using lighter encryption algorithms on this network segment should not compromise the overall security. If you change the default list of preferred ciphers, make sure the specified ciphers are included in the backend servers' list of preferred ciphers as the SSL connection will otherwise be refused. For more information about supported ciphers and cipher list formats, see Appendix A, Supported Ciphers, in the *User's Guide*.
verify
Displays the SSL Connect Verify Settings menu. To view menu options, see /cfg/ssl/server <id> /adv /sslconnect/verify SSL Connect Verify Configuration on page 135.

/cfg/ssl/server <id> /adv/loadbalanc /backend <server id> Backend Server Configuration

```
[Backend Server 1 Menu]
      ip         - Set IP addr of backend server
      port       - Set backend server port
      sslconnect - Set perform SSL connect if enabled for server
      remote     - Set server is remote
      rname      - Set host name of remote server
      remotessl  - Set remote site is ssl
      lbstrings  - Set load balancing strings
      lbop       - Set string load balancing operation
      del        - Remove backend server
      ena        - Enable backend server
      dis        - Disable backend server
```

The Backend Server menu is used for configuring backend servers (also known as "real servers"). The virtual SSL server for which the backend server is configured, can then initiate requests to the enabled backend servers. An index number is assigned to each backend server, and you can create up to 256 backend servers. By specifying an unused index number

when you enter the Backend Server menu, you create a new backend server which can then be configured.

HTTP redirects cannot contain explicit IP addresses because the browser will not be able to verify the server certificates. To solve this problem, one additional virtual server IP (vip) address on each side is introduced. When a client is redirected to the backup site, it is redirected to the name of that local VIP. Each local VIP must have a valid server certificate that matches its name.

To view all backend servers including their current configurations, use the **cur** command in the Load Balancing Settings menu (**/cfg/ssl/server #/adv/loadbalanc**).

Table 39: Backend Server Menu Options (/cfg/ssl/server/adv/loadbalanc /backend)

Command Syntax and Usage
ip <*backend server IP address*>
Sets the IP address of a backend server to which the virtual SSL server can initiate requests.
port <*TCP port number*>
Sets the TCP port to which the virtual SSL server connects when initiating requests. Note that the backend server(s) must be configured to listen for AVG traffic on the TCP port that you specify with this command.
sslconnect on|off
Enables or disables SSL connect on this particular backend server. The default setting for **sslconnect** is **on**.
remote true|false
Specifies whether the current backend server should be indicated as remote. When set to **true**, the IP address of the backend server is matched with the virtual server IP (VIP) address in incoming cookies. The default setting for **remote** is **false**.
rname (host name of remote server)
Specifies the host name of the remote server. The name you specify will be used in the redirect messages.
remotessl true|false
Specifies whether the remote server uses SSL. When the remote server is an HTTPS server, **remotessl** should be set to **true**. This will make the generated redirect an HTTPS redirect even if the local server is an HTTP server. This feature can be used for setting up an HTTP to HTTPS redirect service. The default setting for **remotessl** is **true**.
lbstrings <*index number of match strings*>
Specifies which of the load balancing strings you may have defined that should be mapped to the currently selected backend server. If the virtual SSL server is

Command Syntax and Usage
configured to perform load balancing of backend servers, and the load balancing type is set to **string**, then the specified load balancing metric (Hash, Round Robin, or Least Connections) is applied to the currently selected backend server only for those client requests in which a match of the specified load balancing strings are found. You can also specify negative index numbers, which indicates that a match of the load balancing string represented by the specified index number must not be found in a client request for the backend server to be load balanced.
lbop any|all|one|none
Specifies for which of the load balancing strings you have specified (by using the **lbstrings** command), a match in a client request must be found for the backend server to be load balanced. Valid options are as follows: • **any**: A match of one or more of the specified load balancing strings must be found in a client request for the backend server to be load balanced. • **all**: Matches of all specified load balancing strings must be found in a client request for the backend server to be load balanced. • **one**: A match of one, and only one, of the specified load balancing strings (irrespective which) must be found in a client request for the backend server to be load balanced. • **none**: For the backend server to be load balanced, no match of a specified load balancing string must be found in a client request. If any match is found, the backend server is not load balanced. The default load balancing operation (**lbop**) is `any` .
del
Removes the current backend server, including all its configuration. Before removing a backend server, use the **/cfg/ssl/server #/adv/loadbalanc/cur** command to examine all backend servers by index number and current configuration.
ena
Enables the current backend server. By default, all backend servers are enabled when created.
dis
Disables the current backend server.

/cfg/ssl/server <id> /adv/loadbalanc /remotessl/verify Remote SSL Connect Verify Configuration

```
[Remote SSL Connect Verify Settings Menu]
      verify     - Set certificate verification level
      commonname - Set server common name
      cacerts    - Set list of accepted signers of server's certificate
```

The Remote SSL Connect Verify Settings menu is used for configuring the desired certificate verification level when backend servers are authenticated. The menu is also used to specify the common name of backend servers, as well as setting the CA certificates used for backend server authentication.

Table 40: Remote SSL Connect Verify Settings Menu Options (/cfg/ssl/server/adv/loadbalanc/remotessl/verify)

Command Syntax and Usage
verify none|optional|require Specifies the authentication level to use when establishing an SSL connection towards a backend server. Valid options are as follows: • **none**: No server certificate is required. • **optional**: The server can authenticate by means of a valid certificate but it is not required. • **require**: The server must present a valid certificate in order for the selected virtual SSL server to establish a session. The default value is **none**.
commonname <*common name of backend web server*> Specifies the common name used in the backend server's server certificate. To establish an SSL session, the common name you specify must match the common name found in the certificate used by the backend server(s). The common name found in the server certificate normally corresponds to the name of the web server as it appears in the URL that is used by Internet clients when accessing the web server. Do not include the protocol specifier (**http://**) or any port numbers or pathnames in the common name. Wildcards (such as * or ?) and IP address are not allowed.
cacerts <*CA certificate by index number*> Specifies which of the available CA certificates to use for backend server authentication. To view basic information about all certificates, use the **/info/certs** command. For more information about adding a new CA certificate, see *Avaya VPN Gateway User's Guide*. When specifying more than one certificate, use commas to separate the corresponding index number: Example: 1,2,5

/cfg/ssl/server <number> /adv /sslconnect SSL Connect Configuration

```
[SSL Connect Settings Menu]
      protocol   - Set protocol version
      cert       - Set client certificate
      ciphers    - Set accepted ciphers for ssl connect
      verify     - Verify server menu
      ena        - Enable SSL Connect
      dis        - Disable SSL Connect
```

The SSL Connect Settings menu is used for configuring the SSL protocol, the preferred cipher list, and client authentication for SSL connections between the VPN Gateway(s) and the backend servers.

Table 41: SSL Connect Settings Menu Options (/cfg/ssl/server/adv/sslconnect)

Command Syntax and Usage
protocol ssl2|ssl3|ssl23|tls1|tls11|tls12 Specifies the protocol the virtual SSL server should propose when establishing an SSL session with an SSL-enabled backend server. Valid options are as follows: • **ssl2**: Propose using only SSL 2.0. • **ssl3**: Propose using SSL 3.0 or TLS 1.0. • **ssl23**: Propose using any of SSL 2.0, SSL 3.0, or TLS 1.0. • **tls1**: Propose using only TLS 1.0. • **tls11:** Only accept TLS 1.1. • **tls12:** Only accept TLS 1.2. The default protocol value is **ssl23**.
cert <*client certificate by index number*> Specifies which client certificate the selected virtual SSL server should present to the backend servers, in case the SSL software on the backend servers is configured to require a client certificate. Client authentication is typically very seldom used for SSL connections between the VPN Gateways and the backend servers, as the client is known in these circumstances. To view basic information about available certificates, use the **/info/certs** command. To generate a client certificate, see the "Generating Client Certificates" section in the "Certificates and Client Authentication" chapter in the *User's Guide*.
ciphers <*cipher list format*> Specifies the list of preferred ciphers. This information is sent to the backend servers during the SSL handshake. The default cipher list corresponds to `EXP-RC4-MD5:ALL!DH` , which should be appropriate in most cases. The default cipher list provides for using lighter encryption algorithms between the VPN Gateways and the

Command Syntax and Usage
backend servers than what is normally used between Internet clients and the VPN Gateways. This is desirable mainly in terms of SSL performance. Since both the VPN Gateways and the backend servers typically are behind a firewall in physically secured premises, using lighter encryption algorithms on this network segment should not compromise the overall security. If you change the default list of preferred ciphers, make sure the specified ciphers are included in the backend servers' list of preferred ciphers as the SSL connection will otherwise be refused. For more information about supported ciphers and cipher list formats, see Appendix A, Supported Ciphers, in the *User's Guide*.
verify
Displays the SSL Connect Verify Settings menu. To view menu options, see /cfg/ssl/server <id> /adv /sslconnect/verify SSL Connect Verify Configuration on page 135.
ena
Enables SSL connections between the selected virtual SSL server and configured backend servers. By default, SSL connect is disabled. For greater control, you can disallow SSL connections to a particular backend server by using the **sslconnect** command in the Backend Server menu. For more information, see the **sslconnect** command on sslconnect on|off.
dis
Disables SSL connections between the selected virtual SSL server and all configured backend servers, irrespective of the SSL connect setting on individual backend servers. SSL connect is disabled by default.
cachemode
Lets you enable or disable SSL connections cache mode.

/cfg/ssl/server <id> /adv /sslconnect/verify SSL Connect Verify Configuration

```
[SSL Connect Verify Settings Menu]
      verify     - Set certificate verification level
      commonname - Set server common name
      cacerts    - Set list of accepted signers of server's certificate
```

The SSL Connect Verify Settings menu is used for configuring the desired certificate verification level when backend servers are authenticated. The menu is also used to specify the common name of backend servers, as well as setting the CA certificates used for backend server authentication.

Table 42: SSL Connect Verify Settings Menu Options (/cfg/ssl/server/adv /sslconnect/verify)

Command Syntax and Usage
verify none|require Specifies the authentication level to use when establishing an SSL connection towards a backend server. Valid options are as follows: • None: No server certificate is required. • Require: The server must present a valid certificate in order for the selected virtual SSL server to establish session. The default value is **none**.
commonname <*common name of backend web server*> Specifies the common name used in the backend server's server certificate. To establish an SSL session, the common name you specify must match the common name found in the certificate used by the backend server(s). The common name found in the server certificate normally corresponds to the name of the web server as it appears in the URL used by Internet clients when accessing the web server. Do not include the protocol specifier (http://) or any port numbers or pathnames in the common name. Wildcards (such as * or ?) and IP address are not allowed.
cacerts <*CA certificate by index number*> Specifies which of the available CA certificates to use for backend server authentication. To view basic information about all certificates, use the **/info/certs** command. To add a new CA certificate, see the "Adding certificates to the AVG" section in the "Certificates and Client Authentication" chapter in the *User's Guide*. When specifying more than one certificate, use commas to separate the corresponding index number: Example: 1,2,5

/cfg/cert <id> Certificate Management Configuration

```
[Certificate 1 Menu]
      name       - Set certificate name
      cert       - Set certificate
      key        - Set private key
      revoke     - Revocation menu
      gensigned  - Generate signed client/server certificate
      request    - Generate certificate request
      sign       - Sign a certificate request
      test       - Generate test certificate and key
      import     - Import key and certificate with TFTP/FTP/SCP/SFTP
      export     - Export certificate and key with TFTP/FTP/SCP/SFTP
      display    - Display certificate and key
      show       - Show certificate information
      info       - Show certificate short information
      subject    - Show certificate subject information
      validate   - Check if key and certificate match
      keysize    - Show key size
      keyinfo    - Show how key is stored
      del        - Remove certificate
```

The Certificate menu is used for managing private keys and certificates. When accessing the Certificate menu, you are requested to specify the index number of the certificate you want to work with. When adding a new certificate, specify an unused index number. You can add up to 1500 certificates to the VPN Gateway. Any unused index number can be assigned to a certificate, including numbers higher than 1500. To view basic information about all certificates added to the VPN Gateway, use the **/info/certs** command.

Table 43: Certificate Menu Options (/cfg/cert)

Command Syntax and Usage
name <*certificate name*> Assigns a name to the certificate. The assigned name is mainly for your own reference.
cert Lets you paste the contents of a certificate file from a text editor. If the certificate file contains both the private key and the certificate, you can paste the entire contents at the menu prompt. In this case, you will not need to paste the private key separately using the **key** command. If the key has been password protected, you are prompted for the correct password phrase. When using the **cert** command to add a certificate to the VPN Gateway, the certificate (and key, if present) must be in the PEM format. If a certificate is already installed using the current certificate index number, that certificate will be overwritten by pasting another certificate to the same index number. Use the **show** command to verify that the current certificate index number is not in use.

Command Syntax and Usage
Note: This command cannot be used on an ASA FIPS running in FIPS mode, if the certificate file also contains the private key, or if you need to import the private key associated with the public key in the certificate from an external source. Due to FIPS security requirements, FIPS mode prohibits importing of private keys.
key
Lets you paste the contents of a key file from a text editor. Make sure the key file corresponds to the public key in the related certificate file. If the key has been password protected, you are prompted for the correct password phrase. When using the **key** command to add a private key to the VPN Gateway, the key must be in the PEM format. If a key is already installed using the current certificate index number, that key will be overwritten by pasting another key to the same index number. Use the **keyinfo** command to verify that the current certificate index number is not in use. After you have added the private key you should use the **validate** command to ensure that the private key matches the public key in the current certificate. **Note:** This command cannot be used on an ASA FIPS running in FIPS mode. Due to FIPS security requirements, FIPS mode prohibits importing of private keys.
revoke
Displays the Revocation menu. To view menu options, see /cfg/cert <id> /revoke Certificate Revocation Configuration on page 142.
gensigned server|client *<country> <state or province> <locality> <organization> <organizational unit> <common name> <e-mail address> <subject alternative name> <validity period> <key size> <CA cert [true/false]> <serial number> <pass phrase>*
Generates a server or client certificate that is signed using the private key associated with the currently selected certificate. • **server** : Generates a signed server certificate provided with key use options that are appropriate for server usage. Setting the CA cert value to **true** is appropriate if you plan to issue your own client certificates or chained server certificates, generating them from the currently generated server certificate. The CA cert value you specify when generating a certificate translates into the `X509v3 Basic Constraints` property in the generated certificate. The properties of a certificate available on the VPN Gateway can be viewed by entering the following command: **/cfg/cert #/show** • **client** : Generates a client certificate that is signed using the private key associated with the currently selected certificate. To authenticate a client that is using the generated client certificate, you must also specify the currently selected certificate as a CA certificate to the virtual SSL server handling the authentication for the intended service. For portal servers (used for VPNs), use

Command Syntax and Usage
the **/cfg/vpn <id>/server/ssl/cacerts** command. For virtual SSL servers specified under **/cfg/ssl**, use the **/cfg/ssl/server #/ssl/cacerts** command. Specify the desired CA certificate by its index number. For more information about generating client certificates, see the "Generating Client Certificates" section in the "Certificates and Client Authentication" chapter in the *User's Guide*. **Note:** Only certificates that have the basic constraint `CA:TRUE` can be used to generate server or client certificates. When generating a certificate, the VPN Gateway automatically checks that the currently selected certificate has the basic constraint `CA:TRUE` . **Note:** When generating the certificate, all questions need not be answered. Only one of Common Name and E-mail is strictly required.
request <*country code*> <*state or province*> <*locality*> <*organization*> <*organizational unit*> <*common name*> <*e-mail address*> <*subject alternative name*> <*key size*> <*request CA certificate*>
Generates a certificate signing request (CSR), which can be further processed by a certificate authority (CA) such as VeriSign, Entrust, or any other CA. During the process of generating a CSR, you are asked whether to generate a new private key. The default answer is Yes. However, if you want to generate a CSR using the existing private key, you should answer No. If your existing certificate is reaching its expiration date and you only want to renew it, you should keep using the existing private key and answer No. For more information about how to generate a CSR, see the "Generating and Submitting a CSR Using the CLI" section in the "Certificates and Client Authentication" chapter in the *User's Guide*. **Note:** When generating the certificate signing request, all questions need not be answered. Only one of Common Name and E-mail is strictly required.
sign <*pasted contents of CSR file*>
Signs a CSR (Certificate Signing Request) by using the private key associated with the currently selected certificate. First, open the CSR file in a text editor and copy the entire contents, including the text "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----". Then, after having issued the **sign** command, follow the instructions on screen. **Note:** This command is primarily intended to be used when you have configured the virtual SSL server to perform end to end encryption, and you want to sign a CSR generated on a backend web server by using a CA certificate on the VPN Gateway. (The signed CSR can then be installed on the backend web server

Command Syntax and Usage
as a server certificate). In such a configuration, make sure the certificate you used for signing the CSR is specified as a CA certificate on the virtual SSL server. To set a certificate as a CA certificate used by a particular virtual SSL server, enter the command **/cfg/ssl/server #/adv/sslconnect/verify/cacerts** and specify the index number of the appropriate CA certificate.
test <*country code*> <*state or province*> <*locality*> <*organization*> <*organizational unit*> <*common name*> <*e-mail address*> <*subject alternative name*> <*validity period*> <*key size*>
Generates a self-signed certificate and private key for testing purposes. After providing the requested information, the certificate and key are generated immediately. However, to activate the test certificate and key, you need to execute the **apply** command. **Note:** If a certificate and key already exist for the current certificate index number, they are overwritten when you execute the **apply** command. You should therefore always choose an unused certificate index number before creating a test certificate. To check if a certificate and key already exist for the current index number, use the **info** command. **Note:** When generating the certificate, all questions need not be answered. Only one of Common Name and E-mail is strictly required.
import <*protocol* [tftp|ftp|scp|sftp]> <*server by host name or IP address*> <*file name*>
Installs a private key and certificate by downloading it from a TFTP/FTP/SCP/SFTP server. If the private key has been password protected, you are prompted for the correct password phrase. Keys in the following formats can be imported using the **import** command: PEM, DER, NET, PKCS8 (used in WebLogic), PKCS12, and keys in the proprietary format used in MS IIS 4. Keys from Netscape Enterprise Server or iPlanet Server can also be imported, but require that you first use a conversion tool. Contact Avaya for more information about the conversion tool. Certificates in the following formats can be imported using the **import** command: PEM, DER, NET, PKCS7, and PKCS12. If a key or certificate is already installed using the current certificate index number, that key/certificate will be overwritten by installing another key/certificate to the same index number. Use the **keyinfo** and **show** command respectively, to verify that the current certificate index number is not in use. **Note:** This command cannot be used on an ASA FIPS running in FIPS mode, if the certificate file also contains the private key, or if you need to import the private key associated with the public key in the certificate from an external source. Due to the FIPS security requirements, FIPS mode prohibits importing private keys.

Command Syntax and Usage
export <*protocol* [tftp|ftp|scp|sftp]> <*server by host name or IP address*> <*export file format*[pem|der|net|pkcs12]>
Exports the current key and certificate to a TFTP/FTP/SCP/SFTP server in the specified format. Keys and certificates can be exported and saved into four different formats: PEM, DER, NET, or PKCS12. These formats have different capabilities regarding private key encryption and the ability to save the private key and the certificate in separate files. Only the DER format does not offer private key encryption. The DER format and the NET format lets you store the private key and the certificate in separate files. The PEM format and the PKCS12 format always combine the private key and the certificate in the same file. Most web browsers allow importing a combined key and certificate file in the PKCS12 format. **Note:** When using this command on an ASA FIPS, you can only export the certificate —not the private key. For client certificates however, both the certificate and the private key can be exported to a TFTP/FTP/SCP/SFTP server using the **export** command.
display <*pass phrase*>
Displays the current key and certificate in the CLI. When executing the **display** command, you are provided with the option to protect the private key with a password phrase. This adds an extra layer of security and is recommended. You can perform a cut-and-paste operation on the key section into a text editor, and save the private key to a file with the **.PEM** extension. Repeat the cut-and-paste operation on the certificate section and save it to a file with the **.PEM** extension. You may also save both the key and the certificate to the same file, again using the **.PEM** extension. If you need to save a certificate and key in another format than the PEM format, use the **export** command instead. **Note:** When using this command on an ASA FIPS, only the certificate section is displayed unless the currently selected certificate is a client certificate. For client certificates, both the certificate section and the private key section are displayed and can be saved into a text editor using a cut-and-paste operation.
show
Displays detailed information related to the certificate, except the certificate name.
info
Displays the serial number, the expiration date, and the values specified for the subject part of the current certificate.
subject

Command Syntax and Usage
Displays more detailed information about the subject part of the current certificate, that is . not only the specified values but also the corresponding OIDs (object identifiers) and mnemonic names of each entry. Example: `C/countryName (2.5.4.6) = US` where `countryName` is the mnemonic name, `2.5.4.6` is the OID and `US` is the value.
validate
Validates that the private key matches the public key in the current certificate.
keysize
Displays the key size of the private key in the current certificate.
keyinfo
Provides information about how the private key associated to the currently selected certificate is protected. For the VPN Gateway s without the HSM card, private keys are protected by the cluster. For the ASA FIPS, private keys are protected by the HSM card. However, when generating a client certificate, the associated private key is protected by the cluster and not by the HSM card. This is necessary to transfer both the certificate and the private key to the client using the **export** command.
del
Removes the current certificate and key.

/cfg/cert <id> /revoke Certificate Revocation Configuration

```
[Revocation Menu]
      add         - Add decimal serial number to revocation list
      addx        - Add hex serial number to revocation list
      del         - Cancel revocation for a serial number
      list        - List revoked certificates
      rev         - Enter revocation list
      import      - Import revocation list with TFTP/FTP/SCP/SFTP
      automatic   - Automatic CRL retrieval menu
```

The Certificate Revocation menu is used for revoking client certificates.

Table 44: Certificate Revocation Menu Options (/cfg/cert/revoke)

Command Syntax and Usage
add <*client certificate serial number*> Adds a client certificate, specified by its serial number, to the current certificate revocation list.

Command Syntax and Usage
addx <*client certificate serial number in hexadecimal form*>
Adds a client certificate, specified by its serial number in hexadecimal form, to the current certificate revocation list. When using the **list** command to view revoked certificates, certificates added by using the hexadecimal form are listed using their decimal form.
del <*client certificate serial number*>
Removes a client certificate, specified by its serial number, from the current certificate revocation list. This will cancel the revocation of the specified certificate.
list
Lists the serial numbers of client certificates that will be revoked on client authentication.
rev
Lets you paste the contents of a certificate revocation list in the PEM or ASCII format from a text editor. The revocation list is used to revoke client certificates issued by a particular certificate authority (CA). The currently selected certificate index number (Cert 1, for example) should hold the CA certificate of the same CA as from which you obtained the certificate revocation list. To view information about the currently selected certificate, use the **/cfg/cert #/show** command. If your organization has issued its own client certificates, it may as well have created its own certificate revocation list in ASCII format. Such a list can also be pasted and added to the CA certificate that was used to generate the client certificates.
import <*protocol* [tftp|ftp|scp|sftp]> <*server by host name or IP address*> <*file name*>
Adds a certificate revocation list in PEM, DER or ASCII format by downloading it from a TFTP/FTP/SCP/SFTP server. The revocation list is used to revoke client certificates issued by a particular certificate authority (CA). The currently selected certificate index number (Cert 1, for example) should hold the CA certificate of the same CA as from which you obtained the certificate revocation list. To view information about the currently selected certificate, use the **/cfg/cert #/show** command. If your organization has issued its own client certificates, it may as well have created its own certificate revocation list in ASCII format. Such a list can also be downloaded and added to the CA certificate that was used to generate the client certificates.
automatic
Displays the Automatic CRL menu. To view menu options, see /cfg/cert <id> / revoke/automatic Automatic CRL Menu on page 144.

/cfg/cert <id> /revoke/automatic Automatic CRL Menu

```
[Automatic CRL Menu]
      url         - Set URL to retrieve CRL from
      authDN      - Set LDAP DN used for bind/authentication
      passwd      - Set password to use when to authenticate
      anonymous   - Set LDAP Enable Anonymous login
      interval    - Set refresh interval
      cacerts     - Set list of accepted signers of CRLs
      verify      - Set verification of signed CRL using cacerts
      ena         - Enable automatic retrieval
      dis         - Disable automatic retrieval
```

The Automatic CRL menu is used for configuring access to a server containing CRLs (certificate revocation lists), and retrieving such lists at regular intervals to automate the task of keeping the CRL up-to-date.

Note:

When enabling automatic retrieval of certificate revocation lists, any existing revocation list is overwritten.

You can use LDAP, HTTP, or TFTP to retrieve CRLs from the appropriate server (for LDAP, the server must support LDAP v3). When using LDAP, a bind operation to the specified LDAP server is performed each time a CRL retrieval occurs. The bind operation uses the specified distinguished name and password. Directly after a successful bind operation, a search for the CRL attribute specified in the URL is performed on the LDAP server. For more information on the implementation details behind these operations, see RFC 2251.

Table 45: Automatic CRL Menu Options (/cfg/cert/revoke/automatic)

Command Syntax and Usage
url *<URL with access protocol, server by host name or IP address:TCP port, and path>* Sets the complete URL for retrieving a CRL using LDAP, HTTP, or TFTP. If you are not using the default TCP port of the respective protocol, the TCP port number must also be included in the URL. If you want to retrieve CRLs from an LDAP server, you need to provide the distinguished name of the specific object on the LDAP server, together with the attribute that holds the CRL (all in accordance with RFC 2255). Example: **ldap://10.42.128.30:389/cn=VeriSign CRL,o=Your Organization? CertificateRevocationList;binary** **Note:** RFC 2255 states that entering host information is optional. The AVG software's implementation of the CRL retrieval feature however requires that host information is specified (see preceding example). Using HTTP or TFTP, the URL you specify must include the specific file name you want to access. The recognized URL syntax is a subset of RFC 1738, and can be defined as:

Command Syntax and Usage
<proto>://<host>[:<port>]/<path>. Example: **http://10.42.128.30/server.crl**
authDN <*distinguished name for binding and authentication*>
Sets the distinguished name used for binding and authenticating the initiated LDAP session on the specified LDAP server. Check your LDAP server documentation for details on binding, authentication, and access control. Example: cn=Bill Smith,o=Your Organization When using HTTP or TFTP to retrieve a CRL, you don't need to provide a distinguished name for binding and authentication.
passwd <*password for binding and authentication*>
Sets the password used for binding and authenticating the initiated LDAP session on the specified LDAP server. Check your LDAP server documentation for details on binding, authentication, and access control. When using HTTP or TFTP to retrieve a CRL, you don't need to provide a password for binding and authentication.
anonymous true|false
Lets you enable anonymous binding for automatic CRL retrieval through LDAP. • **true**: The **authDN** and **passwd** commands (see above) can be set to anything, including an empty string. • **false**: The **authDN** and **passwd** commands cannot be set to an empty string. The default value is **false**.
interval <*value in seconds*>
Sets the time interval for retrieving CRLs from the resource you have specified using the **url** command. If you want to specify a time interval in minutes, hours or days, enter an integer directly followed by the letter **m, h,** or **d**. The default interval is 1 day (**1d**). The shortest time interval allowed is 601 seconds (10 minutes and 1 second).
cacerts
Specifies which CA certificates that are valid signers of the certificate revocation lists you retrieve. To get an overview over all available certificates, enter the **/info/certs** command. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified CA certificates, press ENTER when asked to enter certificate numbers, then answer yes to the question if you want to clear the list.
ena

Command Syntax and Usage
Enables automatic retrieval of CRLs. When using the **apply** command the first time after having enabled automatic retrieval of CRLs, a first retrieval is invoked immediately. After that, retrievals will occur at the specified time interval (where the default value is once every 24 hours).
dis
Disables automatic retrieval of CRLs. By default, automatic retrieval is **disabled** .

/cfg/vpn <id> VPN Menu

```
[VPN 1 Menu]
      name       - Set VPN name
      ips        - Set IP addr(s) of the VPN
      standalone - Set standalone mode (no switch)
      aaa        - AAA menu
      server     - SSL server menu
      l2tp       - L2tp server menu
      ipsec      - IPsec server menu
      ippool     - IP address pool menu
      hippool    - Host IP address pool menu
      hostippool - Enable Host IP pool feature
      portal     - Portal look and feel menu
      linkset    - Portal linkset menu
      vdesktop   - Virtual desktop menu
      sslclient  - SSL VPN client menu
      spoclient  - SPO management menu
      adv        - Advanced settings menu
      del        - Remove VPN
```

The VPN menu is the top level in the menu structure designed for VPN deployment. Among other features, it includes options for AAA configuration (Authentication, Authorization, and Accounting), SSL, and IPsec server configuration and Portal layout management.

Table 46: VPN Menu Options (/cfg/vpn)

Command Syntax and Usage
name Assigns a name to the VPN. The name is not used by any other functions but is mainly for your own reference.
ips *<portal IP addresses, comma separated)*
Lets you add one or several portal IP addresses for the current VPN. To access intranet resources from a remote location, the user should connect to the portal IP address for authentication. For SSL connections (HTTPS), the portal IP address (or the corresponding DNS name) should be entered in the client browser's address field. For SSL VPN client connections (SOCKS encapsulated in SSL), the portal IP address or DNS name should be configured in the Avaya SSL VPN client.

Command Syntax and Usage
For IPsec connections, the portal IP address should be configured in the Avaya VPN client (formerly Contivity). If needed, several portal IP addresses can be configured. Below is an example of how to configure two portal IP addresses, using comma separation: 10.1.81.146,192.168.128.212
standalone on|off
When a VPN Gateway (or a cluster of VPN Gateways) is used without being connected to an Application Switch, standalone mode should be enabled. On the other hand, if the VPN Gateway is connected to an Application Switch, standalone mode should be disabled. With this setting, only one IP address can be configured using the ips command (see above). This IP address should be mapped to the corresponding virtual IP address (vip) configured on the Application Switch. Standalone mode is set to on by default.
aaa
Displays the AAA menu for configuring authentication methods, user groups, access rules and so on. To view menu options, see /cfg/vpn <id> /aaa AAA Configuration on page 149.
server
Displays the Server menu for configuring the SSL server used in the current VPN. To view menu options, see /cfg/vpn <id> /server Portal Server Configuration on page 250.
l2tp
Displays the L2TP Menu. For more information about options, see /cfg/vpn <id>/l2tp Layer 2 Tunneling Protocol Configuration on page 273.
ipsec
Displays the IPsec menu for configuring the VPN Gateway to support IPsec connections. To view menu options, see /cfg/vpn <id>/ipsec IPsec Configuration on page 282. **Note:** This command is not available if the VPN Gateway software runs on the ASA 310 or ASA 410 hardware platforms.
ippool
Lets you enter a wizard for creating an IP pool. Once the wizard is completed, the Pool menu is displayed. To view menu options, see /cfg/vpn <id> /ippool <id> IP Pool Configuration on page 307.
hippool <pool name or number> <set pool name> <set proxyarp on|off|all>
The hippool command is available only when **hostippool** is true. Lets you enter a wizard for creating the host IP pool. After the wizard is completed, the Host IP Pool

Command Syntax and Usage
menu appears. For more information about options, see /cfg/vpn <id>/hippool Host IP Pool Configuration on page 313. To view hippool option in the menu, enable **hostippool**.
hostippool true|false
Lets you enable or disable the host IP pool feature in a clustered environment. You can allocate client IP to a particular host in the cluster.
portal
Displays the Portal menu including options for customizing the Portal web page. To view menu options, see /cfg/vpn <id> /portal SSL VPN Portal Configuration on page 316.
linkset
Displays the Linkset menu for defining sets of links to be displayed on the Portal's Home tab. To view menu options, see /cfg/vpn <id> /linkset <id> Linkset Configuration on page 332.
spolclient
Displays the SPO menu used for configuring the Avaya SPO client settings. To view menu options, see /cfg/ vpn <id>/spoclient SPO Client configuration on page 396.
ssloclient
Displays the SSL VPN Client menu used for configuring the Avaya SSL VPN client settings. To view menu options, see /cfg/vpn <id>/sslclient Net Direct and SSL VPN Client Configuration on page 377.
adv
Displays the Advanced menu including options to configure a backend interface and a dedicated DNS server for the current VPN. To view menu options, see /cfg/vpn <id> /adv Advanced VPN Configuration on page 388.
del
Removes the current VPN, including all settings in menus and submenus.
syslog
Displays VPN specific syslog servers.
vdesktop
Displays virtual desktop menu. For more information, see /cfg/vpn <id> /vdesktop Virtual desktop configuration on page 401.

/cfg/vpn <id> /aaa AAA Configuration

```
[AAA Menu]
      quick      - AAA setup wizard
      tg         - TunnelGuard menu
      nap        - Network Access Protection menu
      idlettl    - Set login session idle time
      sessionttl - Set maximum session length
      wholesec   - WholeSecurity menu
      auth       - Authentication menu
      seqauth    - Sequential authentication menu
      authorder  - Set authentication server fallback order
      secauthord - Set sequential secondary authentication server fallback order
      network    - Network access menu
      defauth    - Set Default authentication with fallback support
      service    - Service access menu
      appspec    - Application specific menu
      extspec    - Filename extension specific menu
      filter     - Client filter menu
      group      - Group menu
      defgroup   - Set default group
      anongroup  - Set anonymous group
      defippool  - Set default IP pool
      ssodomains - Single-Sign on enabled domains menu
      ssoheaders - Single-Sign on headers menu
      radacct    - RADIUS accounting menu
      adv        - Advanced settings menu
```

The AAA menu includes commands for accessing features related to authentication, authorization and accounting. You will for example find commands for activating client security validation using Tunnel Guard and WholeSecurity, authentication methods (for example RADIUS, LDAP, NTLM, SiteMinder, local database), access group configuration and RADIUS accounting.

Table 47: AAA Menu Options (/cfg/vpn/aaa)

Command Syntax and Usage
quick Starts the AAA Quick Setup Wizard. The wizard automatically configures 12 default services (see the **/cfg/vpn <id>/aaa/service** command on /cfg/vpn <id> /aaa/service <id> Service Access Configuration on page 218). A trusted account will also be configured as the **trusted** group with the first available group index number. The user name and password supplied in the wizard will create a user in the local database. The user is mapped to the **trusted** group. Members of the **trusted** group are authorized to all networks, services and paths.
tg Displays the Tunnel Guard menu for configuring the VPN Gateway to perform an SRS check on the remote user's machine before allowing access to the intranet. To view menu options, see /cfg/vpn <id> /aaa/tg Tunnel Guard Menu on page 154.
nap

Command Syntax and Usage
Displays NAP Menu. To view the menu options, see /cfg/vpn <id>/aaa/nap NAP Menu on page 158.
idlettl *<value in seconds (s), minutes (m), hours (h) or days (d)>*
Sets the period during which a user's VPN session can be idle before the connection is automatically closed. When closed, the user must provide his or her user name and password to log in again. This option helps prevent allocation of resources on the VPN Gateway for sessions that are no longer active. When 10% of the portal idle timeout is reached, a logout warning window is displayed. The window warns the user about the upcoming logout and offers to refresh the portal connection. If the portal connection is not refreshed, the user is automatically logged out. If the user is logged out, any sub windows or applets (for example port forwarders) opened during the Portal session are automatically closed. The default idle timeout is 15 minutes (15m). The minimum value is 2m (2 minutes) and the maximum value `31d` (31 days). Instead of configuring the idle timeout on VPN level (using this command), you can configure the value per user group (see the **/cfg/vpn <id>/aaa/group #/idlettl** command). When the user logs in, the best idle timeout value configured for the user's different groups and the VPN's timeout value (configured with this command) will be selected.
sessionttl *<value in minutes (m), hours (h) or days (d)>*
Sets the maximum length of a remote user's VPN session. The user will be logged out after this time has expired, regardless if he is active or not. The default value is **infinity** . The minimum value is **2m** (2 minutes) and the maximum value is **31d** (31 days). Instead of configuring the session timeout on VPN level (using this command), you can configure the value per user group (see the **/cfg/vpn <id>/aaa/group <id>/sessionttl** command). When the user logs in, the best session timeout value configured for the user's different groups and the VPN's timeout value (configured with this command) will be selected.
wholesec
Displays the WholeSecurity menu. To view menu options, see /cfg/vpn <id> /aaa/wholesec WholeSecurity Menu on page 164.
auth
Displays the Authentication menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> Authentication Method Configuration on page 165.
seqauth
Displays SeqAuth Menu. To view menu options, see /cfg/vpn <id>/aaa/auth/seqauth Sequential Authentication Menu on page 215.
authorder *<authentication ID numbers, separated by comma>*

Command Syntax and Usage
Sets the preferred order for which the defined authentication methods are applied when a remote user logs in to the Portal. For example, if you have configured RADIUS authentication under authentication ID 1, LDAP authentication under authentication ID 2, Local database authentication under authentication ID 3, you can specify in which order these authentication methods should be applied. When a match of user name and password is found, the other specified authentication methods are ignored. For best performance, enter the authentication ID whose method supports the main bulk of users as the first number. Also, if you use the Local database for authentication, enter that method first because it is performed extremely fast regardless of the number of users in the database. For other methods, the response times may wary depending on the current network load, server performance, number of users in the database and so on. Example from a CLI session: `>> AAA # authorder Current value: 1 Enter auth order (comma separated): 3,2,1` Where number 3 = Local Database, number 2 = LDAP, and number 1 = RADIUS in this example. **Note:** Even if you have defined only one authentication method, the corresponding authentication ID must be specified with the **authorder** command. To view which authentication ID number that corresponds to a currently configured authentication method, use the **/cfg/vpn <id>/aaa/cur** command.
secauthord
Specifies the authentication order. Enter the authentication order separated by comma.
network
Displays the Network menu, after you have typed the index number or name of an existing network or the index number of a new network. To view existing network entries, press TAB following the **network** command. To view menu options, see /cfg/vpn <id> /aaa/network <id> Network Access Configuration on page 216.
defauth on|off
Sets the availability of default fallback based on the authentication used in the authorder. Valid options are as follows: • on: Default Login Service appears in the portal login page. • off: The authentication methods configured in the authorder appear in the login page. The drop-box in the Login page displays these authentication methods in the same authentication order. For all the authentication methods the display name must be set when defauth is off. The default value is **on**.
service

Command Syntax and Usage
Displays the Service menu, after you have typed the index number or name of an existing service or the index number of a new service. To view existing service entries, press TAB following the **service** command. To view menu options, see /cfg/vpn <id> /aaa/service <id> Service Access Configuration on page 218.
appspec
Displays the Appspecific menu, after you have typed the index number or name of an existing appspec entry or the index number of a new appspec entry. To view existing appspec entries, press TAB following the **appspec** command. To view menu options, see /cfg/vpn <id> /aaa/appspec <id> Application Specific Menu on page 220.
extspec <1-1023> <file name extension>
Displays File Extension Specification Menu. To view menu options, see /cfg/vpn <id>/aaa/extspec <1-1023> File Extension Specifications Menu on page 221.
filter
Displays the Client Filter menu, after you have typed the index number or name of an existing filter or the index number of a new filter. To view existing filter entries, press TAB following the **filter** command. To view menu options, see /cfg/vpn <id> /aaa/filter <id> Client Filter Configuration on page 222.
group <*group by ID number or name*>
Displays the Group menu. To view menu options, see /cfg/vpn <id> /aaa/group <id> Group Configuration on page 226.
defgroup <*default group by name*>
Sets an existing user access group that has been defined using the **/cfg/vpn <id>/aaa/group** command as the default user access group. The default group is applied to an authenticated SSL VPN user whose group membership cannot be determined. This typically happens when a match between the user's group membership as specified in the authentication mechanism holding the SSL VPN user's credentials (user name, password, and group membership), and the corresponding group name as specified in the VPN (using the **/cfg/vpn <id>/aaa/group** command) cannot be found. In such a case, the authenticated SSL VPN user will automatically become a member of the specified default group, and the access control lists associated with the default group will determine which rights are granted to the user. **Note:** Because the default group applies to any SSL VPN user whose group membership cannot be determined, make sure that the access control lists associated with the default group do not grant excessive rights.
anongroup <*anonymous group by name*>

Command Syntax and Usage
Lets you reference a previously created user group. Anybody who tries to access a resource through the Portal without prior authentication will be assigned to this group. The access rules of the referenced group determine if access to the requested resource is allowed or not. Example: The remote user requests an intranet web page through the Portal by entering https://vpn.example.com/http/accounting.example.com in the address field, (where vpn.example.com is the Portal address). According to the access rules of the anonymous group, access is only allowed to a specific intranet server used for client security tests. Since access is denied, the Portal's login page is displayed instead. To create a user group with access rules, use the **/cfg/vpn <id>/aaa/group** command.
defippool <*ip pool number*>
Lets you reference 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 VPN client connections and Net Direct client connections. For more information about IP pools, see /cfg/vpn <id> /ippool <id> IP Pool Configuration on page 307.
ssodomains
Displays the SSO (Single-Sign-On) Domains menu. To view menu options, see /cfg/vpn <id> /aaa/ssodomains Single-Sign-On Domain Configuration on page 243.
ssoheaders
Displays the SSO (Single-Sign-On) Headers menu. To view menu options, see /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244.
radacct
Displays the RADIUS Accounting menu. To view menu options, see /cfg/vpn <id> /aaa/service <id> Service Access Configuration on page 218.
adv
Displays Advanced Menu. To view options, see /cfg/vpn <id>/aaa/adv Advanced Group Menu on page 249.

/cfg/vpn <id> /aaa/tg Tunnel Guard Menu

```
[TG Menu]
      ena         - Enable TunnelGuard
      dis         - Disable TunnelGuard
      quick       - Quick TunnelGuard setup wizard
      recheck     - Set recheck interval
      action      - Set fail action
      agent       - Agent settings menu
      list        - List SRS rules
      details     - Display SRS failure details
      runonce     - Run Once mode for TunnelGuard
      logmode     - Logging only mode for TG
      loglevel    - Set TunnelGuard applet loglevel
      bypass      - Bypass TunnelGuard check
```

The Tunnel Guard menu is used to enable Tunnel Guard and to configure global Tunnel Guard settings for the current VPN.

Tunnel Guard is responsible for checking that the required components (executables, DLLs, configuration files, and so on.) necessary to comprise a personal firewall are installed and active on the remote user's machine.

How is Tunnel Guard Activated?

For HTTPS connections (login through Portal), a Tunnel Guard 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 Tunnel Guard agent is activated on the remote user's machine (if installed) when the user logs in to the VPN.

SRS Rules

Which components to look for on the client machine is configurable through a certain specification, a so called SRS rule. The SRS rule in its turn should be mapped to one or more user groups using the **`/cfg/vpn <id>/aaa/group #/tgsrs`** command.

SRS rules can only be defined through the Browser-Based Management Interface (BBI), not through the CLI. See the "Configure Tunnel Guard" chapter in the *Application Guide for VPN*.

When Tunnel Guard is done checking the client machine, it reports the result to the server. If the SRS rule check succeeded (required components were present on the client machine), the user is permitted access to intranet resources as specified in the user group's access rules. If the check failed, the behaviour is configurable. Either the session/tunnel can be torn down or the user may be granted restricted access.

For more information about Tunnel Guard and configuration examples, see the "Configure Tunnel Guard" chapter in the *Application Guide for VPN*.

Table 48: Tunnel Guard Menu Options (/cfg/vpn/aaa/tg)

Command Syntax and Usage
ena Enables Tunnel Guard for the current VPN.
dis Disables Tunnel Guard for the current VPN.
quick Starts the Tunnel Guard configuration wizard. Apart from enabling Tunnel Guard, the wizard creates the following settings: • Two client filters, **tg_passed** and **tg_failed** . The filters are used to trigger different extended profiles, depending on whether the Tunnel Guard checks failed or succeeded. • Two linksets, **tg_passed** and **tg_failed** , for printing the result of the Tunnel Guard checks on the Portal's Home tab. The linkset texts read "The Tunnel Guard checks succeeded!" and "The Tunnel Guard checks failed." respectively. The latter linkset text also includes the variables *<var:tgFailureReason>* and *<var:tgFailureDetail>* who expand to more detailed information about the failure of the Tunnel Guard check (also see the "Variables" section on Variables on page 28). • A test SRS rule called **srs-rule-test** . It checks if the **tg.txt** file is present in the `c:\tunnelguard` folder on the remote user's machine. • A group called **tunnelguard** with two extended profiles. Extended profile 1 is triggered when the Tunnel Guard checks have succeeded. Its access rule gives access to all networks. Extended profile 2 is triggered when the Tunnel Guard checks have failed. It has no access rules which means access is denied to all networks and services. • A Tunnel Guard test user with user name and password `tg` is created and mapped to the **tunnelguard** group. • The SRS rule **srs-rule-test** is mapped to the **tunnelguard** group. • The **tg_passed** linkset is mapped to Extended profile 1. The **tg_failed** linkset is mapped to Extended profile 2. Having run the wizard, you can either edit the settings created by the wizard to create your own Tunnel Guard configuration, or create a completely new configuration based on the information given above. For more information about base profiles, extended profiles and client filters, see the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN*.
recheck *<time in seconds (s), minutes (m) or hours (h)>* Sets the time interval for SRS rule rechecks made by Tunnel Guard 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

Command Syntax and Usage
method, this means that the remote user is kicked out from the Portal or has his IPsec tunnel torn down. The default recheck interval is 15m = 15 minutes. The maximum recheck interval is 24h.
action teardown|restricted
Sets the action to perform when an SRS rule or NAP check fails. That is, action is performed when the components installed or running on the client machine does not fulfill the requirements specified in the SRS rule or NAP Health requirements. • **teardown** . The SSL session/IPsec tunnel is torn down. • **restricted** . The session/tunnel is intact but access should be restricted. Specify limited access rights in the access rules specified for the group's base profile. If the SRS rule check succeeds, an extended profile whose client filter is set to **tg** should be triggered instead. The extended profile's access rights could be more generous. For more information about base profiles, extended profiles and client filters, see the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN*. The default action is `teardown` .
agent
Displays the agents settings menu.
list
Lists all configured SRS rules. **Note:** SRS rules can only be configured through the Browser-Based Management Interface (BBI). See the "Configure Tunnel Guard" chapter in the *Application Guide for VPN*.
details on|off
Lets you specify whether or not Tunnel Guard SRS rule failure details should be displayed to the user. • **on:** The **details** link is displayed on the Portal login page if the Tunnel Guard checks fail and the **action** command (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:tgFailureDetail*> variable. See Variables on page 28 and the "Configure Tunnel Guard" chapter in the *Application Guide* for more information. • **off:** The **details** link is not displayed. The <*var:tgFailureDetail*> variable is not expanded. The default value is **on** .

Command Syntax and Usage
Note: This setting has no impact on the behaviour of the installed Tunnel Guard agent, that is, even if the setting is disabled on the AVG, it might be enabled in the Tunnel Guard agent settings.
runonce on|off
Lets the client to run SRS checks only one time and the resulting access is provided until the session logout. The runonce mode is applicable only for the portal and SPO clients. It also prevents session exit due to heartbeat timeout and rechecks. You can enable or disable this option. The default value is **off**.
logmode on|off
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. The default value is **off**.
loglevel fatal|error|warning|info|debug
Sets the log level for debugging information from the Tunnel Guard applet. The information is displayed in the remote user's Java Console window and can be used to track errors in Tunnel Guard SRS rules. In IE, open the Java Console window from the Tools menu. Select Sun Java Console. In Mozilla and Netscape 7.1, open the Java Console window from the Tools menu. Select Web Development and then Java Console. The debugging information supplied in the Java Console window increases with the selected log level, fatal showing only **fatal** errors, **debug** showing detailed information. Press TAB following the **loglevel** command to view available values. The default value is **info** .
bypass on|off
Lets you bypass the Tunnel Guard checks for client machines with unsupported operating systems (for applet) and client machines without Tunnel Guard installed agent. The default value is **off**.

/cfg/vpn <id> /aaa/tg/agent Agent Settings Menu

```
[Agent settings Menu]
      timeout    - Set Agent Query Timeout Interval
      minver     - Set Agent Minimum Version
```

The Agent Settings menu is used to configure Tunnel Guard agent query timeout interval and Tunnel Guard agent minimum version.

Table 49: Agent Settings Menu Options (/cfg/vpn/aaa/tg/agent)

Command Syntax and Usage
timeout <*value in seconds*> Lets you specify the interval between connection attempts from the Tunnel Guard server (on the VPN Gateway) to the Tunnel Guard client (on the client machine). This setting only applies to clients with the Tunnel Guard application installed not Tunnel Guard applets downloaded from the Portal. The default value is 2s (2 seconds).
minver <*version number as N.N.N.N*> Lets you enter the minimum version of the Tunnel Guard agent. Clients with an older version will not be able to connect to the VPN Gateway. This setting only applies to clients with the Tunnel Guard application installed not Tunnel Guard applets downloaded from the Portal. The default value is 0.0.0.0 , that is, all client versions are allowed.

/cfg/vpn <id>/aaa/nap NAP Menu

```
[NAP Menu]
      autorem     - Set Automatic Remediation
      probation   - Probation Settings
      moreinfo    - Set Troublshooting URL
      pdp         - Set Policy Decision Point
      servers     - Remote Network Policy Servers
      shvs        - System Health Validators
      wshv        - Windows System Health Validator
```

Network Access Protection (NAP) provides system health validation access to the private networks. It provides an integrated way of validating the health state of a network client attempting to connect or communicate on a network. This limits the access of a network client until the health policy requirements are met.

Network Access Protection also allows deployment of NAP clients with or without a Microsoft Network Policy Server (NPS) on the backend network. The Microsoft NPS server is consulted and its response is used in a configurable way to augment the access decision made by the AVG server.

Table 50: NAP Menu options (cfg/vpn <id>/aaa/nap)

Command Syntax and Usage
autorem *true*|*false* You can enable or disable this option. When autorem is enabled, the client tries to remediate itself automatically according to the System health policies. The default value is **false**.
probation

Command Syntax and Usage	
	Displays the Probation Settings Menu. For more information about options, see /cfg/vpn <id>/aaa/nap/probation Probation Settings Menu on page 159.
moreinfo	
	Lets you specify the troubleshooting URL. For example, http://www.example.com/troubleshoot.html.
pdp local|remote	
	Lets you specify Policy Decision Point (PDP) as local or remote. Valid options are: • local: Use the policies specified in the AVG. • remote: use the policies defined on an external Network Policy Server. Default value is local. **Note:** You must configure at least one Remote NPS server to specify PDP.
servers	
	Displays the Network Policy Servers Menu. For more information about options, see /cfg/vpn <id>/aaa/nap/servers Remote Network Policy Servers Menu on page 160.
shvs	
	Displays the System Health Validators Menu. For more information about options, see /cfg/vpn <id>/aaa/nap/shvs System Health Validators Menu on page 161.
wshv	
	Displays the Windows System Health Validators Menu. For more information about options, see /cfg/vpn <id>/aaa/nap/wshv Windows System Health Validators Menu on page 161.

/cfg/vpn <id>/aaa/nap/probation Probation Settings Menu

```
[Probation Settings Menu]
      ena         - Enable full access for a limited time
      dis         - Disable full access for a limited time
      date        - Set Date
      time        - Set Time
```

Table 51: Probation Settings Menu options (cfg/vpn/aaa/nap/probation)

Command Syntax and Usage
ena

Command Syntax and Usage
Enables full access to the private network for limited duration.
dis
Disables full access for limited duration.
date
Lets you specify the date until when full access must be provided
time
Lets you specify the time until when full access must be provided

/cfg/vpn <id>/aaa/nap/servers Remote Network Policy Servers Menu

```
[Remote Network Policy Servers Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

Table 52: Remote Network Policy Servers Menu options (cfg/vpn <id>/aaa/nap/servers)

Command Syntax and Usage
list Lists all the configured values.
del <index number of the entry>
Deletes the index number of the entry.
add <server IP address> <server IP port> <shared secret>
Adds a new value for server IP address, IP port, and shared secret.
insert <index to insert at> <server IP address> <server IP port> <shared secret>
Inserts value for server IP address, IP port, and shared secret to the specified index.
insert <index number to move> <destination index>
Moves the value from specified index number to destination index.

/cfg/vpn <id>/aaa/nap/shvs System Health Validators Menu

```
[System Health Validators Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

Table 53: System Health Validators Menu options (cfg/vpn <id>/aaa/nap/shvs)

Command Syntax and Usage
list Lists all the configured values.
del <index number of the entry> Deletes the index number of the entry.
add <vendor id> <component id> <module name> Adds a new value for vendor ID, component ID, and module name.
insert <index to insert at> <vendor id> <component id> <module name> Inserts value for vendor ID, component ID, and module name to the specified index.
insert <index number to move> <destination index> Moves the value from specified index number to destination index.

/cfg/vpn <id>/aaa/nap/wshv Windows System Health Validators Menu

```
[Windows System Health Validator Menu]
      firewall   - Firewall
      autoupdate - Automatic Updates
      virus      - Virus Protection
      spyware    - Spyware Protection
      secupdates - Security Updates Protection
```

Table 54: Windows System Health Validators Menu options (cfg/vpn <id>/aaa/nap/wshv)

Command Syntax and Usage
firewall on|off Specifies firewall policy.

Command Syntax and Usage
The default value is **on**.
autoupdate on|off
Specifies policy for automatic Windows update configuration. The default value is **on**.
virus
Displays the Virus Protection Menu. For more information about options, see /cfg/vpn <id>/aaa/nap/wshv/virus Virus Protection Menu on page 162.
spyware
Displays the Spyware protection Menu. For more information about options, see /cfg/vpn <id>/aaa/nap/wshv/spyware Spyware Protection Menu on page 163.
secupdates
Displays the Security Updates Protection Menu. For more information about options, see /cfg/vpn <id>/aaa/nap/wshv/secupdates Security Updates Protection Menu on page 163.

/cfg/vpn <id>/aaa/nap/wshv/virus Virus Protection Menu

```
[Virus Protection Menu]
      enabled    - AntiVirus is enabled
      uptodate   - AntiVirus is up to date
```

Table 55: Virus Protection Menu options (cfg/vpn <id>/aaa/nap/wshv/virus)

Command Syntax and Usage
enabled true|false Specifies antivirus configuration. The default value is **false**.
uptodate true|false Specifies if the antivirus is up to date. The default value is **true**.

/cfg/vpn <id>/aaa/nap/wshv/spyware Spyware Protection Menu

```
[Spyware Protection Menu]
      enabled    - AntiSpyware is enabled
      uptodate   - AntiSpyware is up to date
```

Table 56: Spyware Protection Menu options (cfg/vpn <id>/aaa/nap/wshv/spyware)

Command Syntax and Usage
enabled true|false Specifies the antispyware configuration. The default value is **false**.
uptodate true|false Specifies if antispyware is up to date. The default value is **true**.

/cfg/vpn <id>/aaa/nap/wshv/secupdates Security Updates Protection Menu

```
[Security Updates Protection Menu]
      enabled    - Security Updates Protection is enabled
      severity   - Security Updates Severity
      lastsync   - Duration allowed since last sync
      wsus       - Updates from WSUS are allowed
      winupdate  - Updates from Windows Update are allowed
```

Table 57: Security Updates Protection Menu options (cfg/vpn <id>/aaa/nap/wshv/secupdates)

Command Syntax and Usage
enabled true|false Specifies security updates protection. The default value is **false**.
severity critical|important|moderate|low|all Specifies the severity of the missing updates. The default value is **important**.
lastsync Specifies the duration allowed for the last sync. The default value is **need info**.
wsus true|false

Command Syntax and Usage
Specifies the updates from the Windows Software Update Server (WSUS). The default value is **true**.
winupdate true|false
Specifies if Windows security policies are up to date. The default value is **true**.

/cfg/vpn <id> /aaa/wholesec WholeSecurity Menu

```
[WholeSecurity Menu]
      quick      - WholeSecurity setup wizard
      url        - Set WholeSecurity deployment URL
      logouturl  - Set redirect URL on logoff
      ena        - Enable WholeSecurity
      dis        - Disable WholeSecurity
```

The WholeSecurity menu is used to enable a scan of the remote user's machine to identify any eavesdropping threats, including Trojan horses, remote 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 automatically redirected to a Symantec WholeSecurity Confidence Online server. The Confidence Online software is downloaded to the endpoint machine and performs 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, quarantined and reported.

The configuration on the AVG is limited to enabling WholeSecurity, specifying the URL to a WholeSecurity Confidence Online server and configuring a user access group that allows redi>rection to an intranet web site prior to logging in to the VPN. See the "WholeSecurity" chapter in the *Application Guide for VPN*.

The rest of the configuration is done in 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. See the Confidence Online manual.

Table 58: WholeSecurity Menu Options (/cfg/vpn/aaa/wholesec)

Command Syntax and Usage
quick <*WholeSecurity server name*> <*WholeSecurity deployment name*> Lets you run a wizard for enabling WholeSecurity and specifying all the information required for a fully functioning WholeSecurity setup. See the *Application Guide for VPN* for instructions on what information to supply in the wizard.
url <*URL*> Lets you enter a URL to the WholeSecurity Confidence Online server, according to the following format: https://<confidence_online_server>/llclient /<deployment>/online.html.

Command Syntax and Usage
For example, if the Confidence Online server is running at confidence.example.com and the deployment is called AvayaSSLVPN, the resulting URL would be: https://confidence.example.com/llclient/AvayaSSLVPN/online.html
logouturl <URL>
The URL to which the remote user will be redirected on logoff. When WholeSecurity is enabled, the Login page will not be displayed when the user logs out from the Portal session.
ena
Enables WholeSecurity (disabled by default).
dis
Disables WholeSecurity.(disabled by default).

/cfg/vpn <id> /aaa/auth <id> Authentication Method Configuration

```
 [Authentication 1 Menu]
type - Set authentication mechanism
name - Set auth name
display    - Set auth display name
domain     - Set windows domain for backend single sign-on
radius     - RADIUS settings menu
ldap - LDAP settings menu
ntlm - NTLM settings menu
siteminder - Netegrity SiteMinder settings menu
cleartrust - RSA ClearTrust settings menu
rsa        - RSA SecurID menu
local- Local database menu
http       - HTTP authentication menu
cert - Client Certificate settings menu
adv  - Advanced settings menu
ena  - Enable Authentication
dis  - Disable Authentication
del  - Remove Authentication
```

The Authentication menu is used to configure one or more authentication methods by which remote users can be authenticated in the current VPN.

After having defined the desired authentication methods, you should also specify in which order the methods should be applied when a user logs in to the VPN, using the **/cfg/vpn <id>/aaa/authorder** command.

Note:

Not all menu items appear; the **radius, ldap, ntlm, siteminder, cleartrust, rsa, local** and **cert** options each appear only when they are selected as the authentication mechanism.

Each authentication method you define corresponds to a specific authentication ID. To view which authentication IDs that are currently in use, press Tab after having typed the **/cfg/vpn <id>/aaa/auth** command.

Table 59: Authentication Menu Options (/cfg/vpn/aaa/auth)

Command Syntax and Usage
type radius|ldap|ntlm|siteminder|cleartrust|rsa|cert|local|http Lets you select an authentication mechanism to configure for the current VPN. The selected mechanism is mapped to the current authentication ID.
name Lets you specify a name for the current authentication method. This name can be selected in a client filter to be used as a condition for extended access rights for group members who has authenticated to this server. For more information about client filters, see /cfg/vpn <id> /aaa/filter <id> Client Filter Configuration on page 222.
display Lets you specify a display name for the current authentication method. The name is displayed in the Login Service list box on the Portal login page and in the Avaya SSL VPN client's login window. The user can thus select a specific authentication server, for example for token authentication or direction to a specific Windows domain. If the user selects **default** in the Login Service list box, authentication will be carried out according to the configured authentication order.
domain Lets you specify an NTLM domain name for the current authentication method. The domain name is used in automatic login links (**iauto**) where the target backend server requires a Windows domain. For more information about these link types, see /cfg/vpn <id> /linkset <id> /link <id> Link Configuration on page 333. When you specify an automatic login link to a web page, the *<var:domain>* macro can be included in the link. When the remote user clicks the link on the Portal's Home tab and the target backend server requires a Windows domain (along with user name and password), the *<var:domain>* macro expands to the domain name specified with this command. If your configuration does not require a Windows domain to be specified for the current authentication method, leave this setting blank.
radius Displays the RADIUS menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /radius RADIUS Configuration on page 169. **Note:** The **radius** menu item is only available when the authentication mechanism is set to **radius**.

Command Syntax and Usage
ldap
Displays the LDAP menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /ldap LDAP Configuration on page 180. **Note:** The **ldap** menu item is only available when the authentication mechanism is set to **ldap**.
ntlm
Displays the NTLM menu. To view menu options, see /cfg/vpn <id> /auth <id> /ntlm NTLM Configuration on page 191. **Note:** The **ntlm** menu item is only available when the authentication mechanism is set to **ntlm**.
siteminder
Displays the SiteMinder menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /siteminder SiteMinder Configuration on page 193. **Note:** The **siteminder** menu item is only available when the authentication mechanism is set to **siteminder**.
cleartrust
Displays the ClearTrust menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /cleartrust ClearTrust Configuration on page 198. **Note:** The **cleartrust** menu item is only available when the authentication mechanism is set to **cleartrust**.
rsa
Displays the RSA SecurID menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /rsa RSA SecurID Configuration on page 203. **Note:** The **rsa** menu item is only available when the authentication mechanism is set to **rsa**.
local
Displays the Local database menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /local Local Database Configuration on page 204.

Command Syntax and Usage
Note: The **local** menu item is only available when the authentication mechanism is set to **local**.
http
Displays the HTTP menu. To view menu options, see /cfg/vpn <id>/aaa/auth <id>/http HTTP authentication on page 207. **Note:** The **http** menu item is available only when the authentication mechanism is set to **http**.
cert
Displays the Cert menu. To view menu options, see /cfg/vpn <id>/aaa/auth <id>/cert Client Certificate Authentication on page 208. **Note:** The **cert** menu item is only available when the authentication mechanism is set to **cert**.
adv
Displays the Advanced settings menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /adv Advanced Settings Configuration on page 212.
ena
Enables Client certificate authentication. To view the settings required for Client certificate authentication, see /cfg/vpn <id>/aaa/auth <id>/cert Client Certificate Authentication on page 208. **Note:** The **ena** menu item is only available when the authentication mechanism is set to **cert**.
dis
Disables Client certificate authentication. **Note:** The **dis** menu item is only available when the authentication mechanism is set to **cert**.
del
Removes all settings for the current authentication ID.

/cfg/vpn <id> /aaa/auth <id> /radius RADIUS Configuration

```
 [RADIUS Menu]
servers    - RADIUS servers menu
vendorid   - Set vendor id for group attribute
vendortype - Set vendor type for group attribute
vpnid- Set vendor id for VPN ID attribute
vpntype    - Set vendor type for VPN ID attribute
timeout    - Set RADIUS server timeout
idletimeou - Idle Timeout menu
sessiontim - Session Timeout Menu
macro- User-defined Macro menu
netattr    - Tunnel network attributes menu
filtattr    - Tunnel filter attributes menu
```

The RADIUS menu is used for configuring remote authentication of users in the VPN by way of the RADIUS (Remote Access Dialup User Service) control protocol as defined in RFC 2865. The menu is also used for accessing the RADIUS servers menu, where the actual RADIUS servers used for remote authentication of users can be specified.

To access the RADIUS menu, the authentication type for the current authentication ID must be set to **radius**.

Table 60: RADIUS Menu Options (/cfg/vpn/auth/radius)

Command Syntax and Usage
servers Displays the RADIUS Servers menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /radius/servers RADIUS Servers Menu on page 171.
vendorid <*integer value*> Assigns the SMI Network Management Private Enterprise Code as defined by IANA in the file http://www.iana.com/ to the Vendor-Id attribute. The Vendor-Idrepresented by the private enterprise numberis a value for RADIUS' standard attribute **vendor-specific** (26). The default Vendor-Id is 1872 (Alteon). **Note:** If another Vendor-Id is used by your RADIUS system, you can use the **vendorid** command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. **Note:** If you want to use a standard attribute type (as defined in RFC 2865) set vendorid to 0. Then configure the desired standard attribute type as the vendor type value

Command Syntax and Usage
(see next command). For example, to use the standard attribute Class, set vendorid to 0 and vendortype to 25.
vendortype <*integer value*>
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 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. VPN group names and access rules are defined using the **/cfg/vpn <id>/aaa/group <id>** command. The default Vendor-Type value is 1. The usage of the Vendor-Type attribute conforms to the recommendations in RFC 2865, section 5.26. **Note:** If another number for **vendor type** is used by your RADIUS system, you can use the vendortype command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. **Note:** If **vendorid** is set to 0, **vendortype** should be set to a standard attribute type as defined in RFC 2865. For example, to use the standard attribute Class, set **vendorid** to 0 and **vendortype** to 25.
vpnid
Sets the Vendor-Id for the VPN ID attribute. When a user authenticates to a specific VPN (as configured on the AVG), the AVG sends the VPN ID to the RADIUS server. The RADIUS server in its turn can make use of the VPN ID to return user information (for example from a VPN-specific user database). The Vendor-Id should correspond to the Vendor-Id used by your RADIUS server. The default Vendor-Id value is `1872` (Alteon). 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 attribute type as defined in RFC 2865, set **vpnid** to 0. Then set **vpntype** to the desired standard attribute (see next command).
vpntype
Sets the Vendor-Type value for the VPN ID attribute. Used in combination with the Vendor-Id, the Vendor-Type number identifies the VPN to which the remote user has logged in. The default Vendor-Type value is set to 3. If your RADIUS server uses another Vendor-Type number, you can change this value. Contact your RADIUS server administrator for more information. If **vpnid** is set to 0, **vpntype** should be set to a standard attribute type as defined in RFC 2865.
timeout <*value in seconds*>

Command Syntax and Usage
Sets a timeout value in seconds for a connection request to a RADIUS server. If the timeout value elapses before a connection is established, authentication will fail. The default RADIUS server timeout value is 10s (10 seconds).
idletimeou
Displays the Idle Timeout menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /radius/idletimeou Idle Timeout Configuration on page 172.
sessiontim
Displays the Session Timeout menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /radius/sessiontim Session Timeout Configuration on page 174.
macro
Displays the Macro menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /radius/macro RADIUS Macro Configuration on page 175.
netattr
Displays the Tunnel network attributes menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /radius/netattr RADIUS Network Attributes Configuration on page 176.
filtattr
Displays the Tunnel filter attributes menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /radius/filtattr RADIUS Filter Attributes Configuration on page 179.

/cfg/vpn <id> /aaa/auth <id> /radius/servers RADIUS Servers Menu

```
 [RADIUS servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The RADIUS Servers menu enables you to list the configured RADIUS servers, delete a RADIUS server, or add a new RADIUS server to the VPN configuration.

To enable RADIUS authentication using the servers added to the list, make sure that the authentication ID that represents the RADIUS configuration is specified using the **/cfg /vpn <id>/aaa/authorder** command.

Table 61: RADIUS Servers Menu Options (/cfg/vpn/aaa/auth/radius/servers)

Command Syntax and Usage
list Displays all RADIUS servers that are added to the RADIUS configuration in the current VPN. The servers are listed by their respective index number, IP address, and shared secret.
del *<RADIUS server by index number>*
Removes the specified server from the VPN. Use the **list** command to display the index numbers of all added RADIUS servers.
add *<IP address of RADIUS server> <TCP port number> <shared secret>*
Adds a RADIUS server to the VPN. Specify the IP address, a TCP port number, and the shared secret. The next available index number is assigned automatically by the system. A maximum of three RADIUS servers can co-exist in the configuration. **Note:** The default port number used by the RADIUS protocol is 1812.
insert *<index number to insert at> <IP address of RADIUS server to add>*
Assigns a specific index number to the RADIUS server you add. The index number you specify must be in use. RADIUS servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move *<index number to move> <destination index number>*
Moves a RADIUS server up or down in the list of configured servers. The index number you specify must be in use. To view all RADIUS servers currently added to the VPN, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /radius/idletimeou Idle Timeout Configuration

```
[Idle Timeout Menu]
vendorid   - Set vendor id for idle timeout attribute
vendortype - Set vendor type for idle timeout attribute
ena  - Enable Idle-Timeout
dis  - Disable Idle-Timeout
```

The Idle Timeout menu 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.

Table 62: Idle Timeout Menu Options (/cfg/vpn/aaa/auth/radius/idletimeou)

Command Syntax and Usage
vendorid <*integer value*> Assigns the SMI Network Management Private Enterprise Code—as defined by IANA in the file http://www.iana.org/—to the Vendor-Id attribute. The Vendor-Id—represented by the private enterprise number—is a value for RADIUS' standard attribute **vendor-specific** (26). Contact your RADIUS system administrator for information about which value to use. If you want to use a standard attribute type as defined in RFC 2865, set **vendorid** to **0**. Then configure the desired standard attribute type as the vendor type value (see next command). **Note:** If both Vendor-Id and Vendor-Type is set to 0, the VPN Gateway will pick up the Idle-Timeout standard attribute (if sent from the RADIUS server). If vendor-specific attributes are specified on the RADIUS server and in the CLI (using Vendor-Id and Vendor-Type), the standard attribute will be overridden.
vendortype <*integer value*> 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 idle timeout attribute configured in RADIUS. The usage of the Vendor-Type attribute conforms to the recommendations in RFC 2865. Contact your RADIUS system administrator for information about which value to use. **Note:** If both Vendor-Id and Vendor-Type is set to 0, the VPN Gateway will pick up the Idle-Timeout standard attribute (if sent from the RADIUS server). If vendor-specific attributes are specified on the RADIUS server and in the CLI (using Vendor-Id and Vendor-Type), the standard attribute will be overridden.
ena Enables retrieval of the RADIUS server idle timeout value. The feature is enabled by default.
dis Disables retrieval of the RADIUS server idle timeout value. By default, the feature is enabled.

/cfg/vpn <id> /aaa/auth <id> /radius/sessiontim Session Timeout Configuration

```
 [Session Timeout Menu]
vendorid   - Set vendor id for session timeout attribute
vendortype - Set vendor type for session timeout attribute
ena        - Enable Session-Timeout
dis  - Disable Session-Timeout
```

The Session Timeout menu 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.

Table 63: Session Timeout Menu Options (/cfg/vpn/aaa/auth/radius/sessiontim)

Command Syntax and Usage
vendorid <*integer value*> Assigns the SMI Network Management Private Enterprise Code—as defined by IANA in the filehttp://www.iana.org/ —to the Vendor-Id attribute. The Vendor-Id—represented by the private enterprise number—is a value for RADIUS' standard attribute **vendor-specific** (26). Contact your RADIUS system administrator for information about which value to use. If you want to use a standard attribute type as defined in RFC 2865, set **vendorid** to **0**. Then configure the desired standard attribute type as the vendor type value (see next command). **Note:** If both Vendor-Id and Vendor-Type is set to 0, the VPN Gateway will pick up the Session-Timeout standard attribute (if sent from the RADIUS server). If vendor-specific attributes are specified on the RADIUS server and in the CLI (using Vendor-Id and Vendor-Type), the standard attribute will be overridden.
vendortype <*integer value*> 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 session time-out attribute configured in RADIUS. The usage of the Vendor-Type attribute conforms to the recommendations in RFC 2865. Contact your RADIUS system administrator for information about which value to use.

Command Syntax and Usage
Note: If both Vendor-Id and Vendor-Type is set to 0, the VPN Gateway will pick up the Session-Timeout standard attribute (if sent from the RADIUS server). If vendor-specific attributes are specified on the RADIUS server and in the CLI (using Vendor-Id and Vendor-Type), the standard attribute will be overridden.
ena
Enables retrieval of the RADIUS server session timeout value. The feature is disabled by default.
dis
Disables retrieval of the RADIUS server session timeout value. The feature is disabled by default.

/cfg/vpn <id> /aaa/auth <id> /radius/macro RADIUS Macro Configuration

```
 [Macro Menu]
list - List all values
del  - Delete a value by number
add        - Add a new value
insert     - Insert a new value
move - Move a value by number
```

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

Example: Map an arbitrary variable name (for example exchangeServer) to a RADIUS user attribute identifying an Exchange server. Create an internal 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.

Table 64: Macro Menu Options (/cfg/vpn/aaa/auth/radius/macro)

Command Syntax and Usage
list Displays all RADIUS macros that are added to the configuration in the current VPN. The macros are listed by their respective index number.
del <*macro by index number*>

Command Syntax and Usage
Removes the specified macro. Use the **list** command to display the index numbers of all added macros.
add *<variable name> <vendor id> <vendor type> <attribute type string|integer|ipaddr>*
Adds a RADIUS macro to the configuration. • Variable name, e.g. **exchangeServer**. By mapping the variable name to the RADIUS attribute (see below), the corresponding value can be retrieved from the logged in user's user record in RADIUS. • Vendor-Id. Lets you specify the Vendor-Id number to be used when retrieving the value from the user record. For more information about Vendor-Id, see /cfg/vpn <id> /aaa/auth <id> /radius/idletimeou Idle Timeout Configuration on page 172. • Vendor-Type. Lets you specify the Vendor-Type number that identifies the user attribute whose value should be retrieved. For more information about the Vendor-Type attribute, see /cfg/vpn <id> /aaa/auth <id> /radius/idletimeou Idle Timeout Configuration on page 172. • Attribute type, i.e **string, integer** or **ipaddr**. Lets you specify the type of value to be retrieved.
insert *<index number to insert at> <macro to add>*
Assigns a specific index number to the RADIUS macro you add. The index number you specify must be in use. Macros with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move *<index number to move> <destination index number>*
Moves a macro up or down in the list of configured macros. The index numbers you specify must be in use. To view all macros currently added to the system configuration, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /radius/netattr RADIUS Network Attributes Configuration

```
[Radius Network Attributes Menu]

clntipid          - Set vendor id for client IP address attribute

clntiptype        - Set vendor type for client IP address attribute
```

```
clntmaskid          - Set vendor id for client netmask attribute

clntmaskty          - Set vendor type for client netmask attribute

primnbnsid          - Set vendor id for primary NBNS server attribute

primnbnsty          - Set vendor type for primary NBNS server attribute

secnbnsid           - Set vendor id for secondary NBNS server attribute

secnbnstyp          - Set vendor type for secondary NBNS server attribute

primdnsid           - Set vendor id for primary DNS server attribute

primdnstyp          - Set vendor type for primary DNS server attribute

secdnsid            - Set vendor id for secondary DNS server attribute

secdnstype          - Set vendor type for secondary DNS server attribute

domainid            - Set vendor id for domain name attribute

domaintype          - Set vendor type for domain name attribute

ena                 - Enable Radius Network Attribute

dis                 - Disable Radius Network Attribute
```

The RADIUS Network Attributes menu is used to 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.

If you want to use a standard attribute type (as defined in RFC 2865), set the vendor id to 0. Then configure the desired standard attribute type as the vendor type value.

Example: Set **clntipid** (vendor id for client IP address attribute) to 0. Then set **clntiptype** to 8 (Framed-IP-Address attribute type).

Table 65: RADIUS Network Attributes Menu Options (/cfg/vpn/aaa/auth/radius/netattr)

Command Syntax and Usage
clntipid

Command Syntax and Usage
Sets the vendor id for the client IP address attribute. The default value is 1872 (alteon).
clntiptype
Sets the vendor type for the client IP address attribute. The default value is 4.
clntmaskid
Sets the vendor id for the client netmask attribute. The default value is 1872 (alteon).
clntmaskty
Sets the vendor type for the client netmask attribute. The default value is 5.
primnbnsid
Sets the vendor id for the primary NBNS server (NetBIOS Name Server) attribute. NBNS servers provide WINS (Windows Internet Naming Service) which is part of the Microsoft Windows NT server environment. The default value is 1872 (alteon).
primnbnsty
Sets the vendor type for the primary NBNS server attribute. The default value is 6.
secnbnsid
Sets the vendor id for the secondary NBNS server attribute. The default value is 1872 (alteon).
secnbnstyp
Sets the vendor type for the secondary NBNS server attribute. The default value is 7.
primdnsid
Sets the vendor id for the primary DNS server attribute. The default value is 1872 (alteon).
primdnstyp
Sets the vendor type for the primary DNS server attribute. The default value is 8.
secdnsid
Sets the vendor id for the secondary DNS server attribute. The default value is 1872 (alteon).
secdnstype

Command Syntax and Usage
Sets the vendor type for the secondary DNS server attribute. The default value is 9.
domainid
Sets the vendor id for the domain attribute. The default value is 1872 (alteon).
domaintype
Sets the vendor type for the domain attribute. The default value is 11.
ena
Enables the settings made on the RADIUS network attributes menu. For the settings to take effect, the **/cfg/vpn <id>/ippool <id>/type** command should be set to **radius**. Disabled by default.
dis
Disables the settings made on the RADIUS network attributes menu. Disabled by default.

/cfg/vpn <id> /aaa/auth <id> /radius/filtattr RADIUS Filter Attributes Configuration

```
[RADIUS Filter Attributes Menu]
      filterid   - Set vendor id for filter attribute
      filtertype - Set vendor type for filter attribute
      ena        - Enable RADIUS Filter Attribute
      dis        - Disable RADIUS Filter Attribute
```

The RADIUS File Attributes menu is used to configure the VPN Gateway to retrieve the filter attributes from an external RADIUS server. AVG takes filter information from RADIUS, and applies the filter to the user tunnel.

Table 66: RADIUS Filter Attributes Menu Options (/cfg/vpn/aaa/auth/radius/filtattr)

Command Syntax and Usage
filterid
Sets the vendor id for the filter attribute.
filtertype
Sets the vendor type for the filter attribute.

Command Syntax and Usage
ena
Enables RADIUS filter attribute.
dis
Disables RADIUS filter attribute.

/cfg/vpn <id> /aaa/auth <id> /ldap LDAP Configuration

```
[LDAP Menu]
quick      - LDAP setup wizard
servers    - LDAP servers menu
servername - LDAP servers menu
searchbase - Set search base entry
groupattr  - Set LDAP group attribute
userattr   - Set LDAP user attribute
isdbinddn  - Set iSD bind DN
isdbindpas - Set iSD bind password
ldapmacro  - User-defined macro menu
enaldaps   - Set Enable LDAPS
enauserpre - Set Enable user preferences
enacutdoma - Set Enable cut domain from user name
enashortgr - Enable short group format
timeout    - Set LDAP server timeout
groupsearc - Group Search settings menu
activedire - Active Directory settings menu
adv  - Advanced settings menu
```

The LDAP menu is used for configuring remote authentication of users in the VPN by way of the Lightweight Directory Access Protocol (LDAP). The menu is also used for accessing the LDAP Servers menu, where the actual servers used for remote authentication of users can be specified.

To access the LDAP menu, the authentication type for the current authentication ID must be set to **ldap**.

Table 67: LDAP Menu Options (/cfg/vpn/aaa/auth/ldap)

Command Syntax and Usage
quick
Lets you set the LDAP sever vendor — microsoft, novel, sun, or other.
servers
Displays the LDAP Servers menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /ldap/servers LDAP Servers Menu on page 183.
servernames

Command Syntax and Usage
Displays the LDAP server names menu. To view menu options, see /cfg/vpn <id> / aaa/auth <id> /ldap/servernames LDAP Server names Menu on page 185.
searchbase <*searchbase entry*>
Method 1: Assigns the DN (Distinguished Name) that points to the entry that is one level up from where all user entries are found. Example: A searchbase value set to ou=People,dc=bluetail,dc=com implies that authentication will be performed against a DN that corresponds to the following: uid = <user> , ou = People, dc = bluetail, and dc = com (where uid is an example of a user attribute, ou = organization unit, and dc = domain component). The **isdbinddn** and **isdbindpas** commands should not be used. Method 2: If user entries are located in several different places in the LDAP Dictionary Information Tree (DIT) or if the user's login name (used to login to the VPN portal) is different from the user record identifier (RDN), the DIT has to be searched. The DN assigned here should point to a position in the DIT from where all user records can be found, using a subtree search. To be able to search the DIT, the VPN Gateway must authenticate itself towards the LDAP server, according to the settings made with the **isdbinddn** and **isdbindpas** commands.
groupattr <*group attribute names, separated by comma*>
Defines the LDAP attribute that contains the name(s) of the group(s) of which a particular user in the VPN is a member. The group names in the LDAP attribute must be defined in the VPN, complete with one or more access control lists. VPN group names and access control lists are defined by using the **/cfg/vpn <id>/aaa/group <id>** command. If you specify more than one group attribute name, separate the names with comma (,).
userattr <*user attribute name*>
Method 1: Defines the LDAP attribute that contains the user name used for authenticating a user in the VPN. The default user attribute name is `uid` . Method 2: If the user's portal login name is not identical with the user record identifier (RDN), for example when using LDAP for authentication towards Active Directory, the LDAP Dictionary Information Tree (DIT) has to be searched for the user record, using a combination of the user's login name and a user attribute. Example: In Active Directory, a user record is defined as the following DN (Distinguished Name): cn=Bill Smith, ou=people, dc=bluetail, dc=com . It also contains the attribute sAMAccountName with the value bill , which corresponds to the user's login name. Thus, if userattr is defined as **sAMAccountName**, the user record Bill Smith will be found. To be able to search the DIT, the VPN Gateway must authenticate itself towards the LDAP server, according to the settings made with the **isdbinddn** and **isdbindpas** commands.
isdbinddn

Command Syntax and Usage
Points out an entry in the LDAP server used for authenticating the VPN Gateway. This command is only used with Method 2.
isdbindpas
Sets the password to be used when the VPN Gateway authenticates to the LDAP entry pointed out with the **isdbinddn** command. This command is only used with Method 2.
ldapmacro
Displays the LDAP Macro menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /ldap/ldapmacro LDAP Macro Configuration on page 186.
enaldaps true|false
By setting this command to **true** , LDAP requests between the VPN Gateway and the LDAP server will be made using a secure SSL connection, that is, LDAPS. When applying the changes, a warning message will be displayed if the LDAP server ports are not the standard LDAPS ones (that is, 636). The default value is **false** .
enauserpre true|false
Enables/disables storage of user preferences in an external LDAP/Active Directory database. • **true.** Storage/retrieval of user preferences is enabled. When the remote user logs out from a Portal session, the VPN Gateway saves any user preferences accumulated during the session in the **isdUserPrefs** attribute. The next time the user successfully logs in through the Portal, the VPN Gateway retrieves the LDAP attribute that holds the user preference data from the LDAP database. • **false.** Storage/retrieval of user preferences is disabled. In the current version, Portal bookmarks and HTTP auto-login information is saved as user preference data. If a user has logged in to a backend server during a Portal session, this login information is saved in the user preference attribute. The next time the user logs in to the Portal and tries to access the password-protected web page, he or she will be logged in automatically. Portal bookmarks saved during a Portal session will be available the next time the user logs in. To support storage/retrieval of user preferences, the LDAP server needs to extend its schema with one new ObjectClass and one new Attribute. For instructions, see Appendix H, "Adding User Preferences Attribute to Active Directory", in the *User's Guide*. The default value is **false.**
enacutdomain true|false
• **true:** Strips the domain part from the login user name before LDAP authentication is performed. Example: If the login user name is

Command Syntax and Usage
john@example.com, the @example.com part will be cut off before LDAP authentication takes place. • **false:** The domain name will not be cut off. The default value is **false.**
enashortgr true|false
Lets you configure the AVG to extract the first part of a returned Distinguished Name (DN) as the group name to be used. This makes it easier to configure the group name in the VPN as you do not have to configure the entire DN string as group name. • **true:** Enables extraction of the first part of the DN as group name. Example: If the DN reads `cn=My Group,cn=User,dc=Company,dc=com, "My Group "` will be used as group name. • **false:** The entire DN string has to be configured as group name in the CLI/BBI if returned as group name from the authentication server. Also see the Group Configuration section on /cfg/vpn <id> /aaa/group <id> Group Configuration on page 226. The default value is **false**.
timeout <*value in seconds*>
Sets a timeout value in seconds for a connection request to an LDAP server. If the timeout value elapses before a connection is established, authentication will fail. The default LDAP server timeout value is 5 seconds.
groupsearc
Displays the LDAP Group Search menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /ldap/groupsearc Group Search Configuration on page 187.
activedire
Displays the Active Directory menu. To view menu options, see /cfg/vpn <id>/aaa/auth <id>/ldap/activedire Active Directory Settings Configuration on page 189.
adv
Displays the Advanced LDAP menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /ldap/adv Advanced LDAP Menu on page 190.

/cfg/vpn <id> /aaa/auth <id> /ldap/servers LDAP Servers Menu

The LDAP server names menu enables you to list the configured LDAP servers, delete an LDAP server, or add a new LDAP server to the Portal configuration by DNS name.

```
[LDAP servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Inserta new value
move - Move a value by number
```

Table 68: LDAP Servers Menu Options (/cfg/vpn/aaa/auth/ldap/servers)

Command Syntax and Usage
list Displays all LDAP servers that are added to the LDAP configuration in the current VPN. The servers are listed by their respective index number and IP address.
del <*LDAP server by index number*>
Removes the specified LDAP server from the VPN configuration. Use the **list** command to display the index numbers of all added LDAP servers.
add <*IP address of LDAP server*> <*TCP port number*>
Adds an LDAP server to the VPN. Specify the IP address of the LDAP server, and a TCP port number. The next available index number is assigned automatically by the system. A maximum of three LDAP servers can co-exist in the configuration. **Note:** The default port number used by the LDAP protocol is 389. If LDAPS is enabled (using the **/cfg/vpn <id>/aaa/auth <id>/ldap/enaldaps** command) change the port number to 636.
insert <*index number to insert at*> <*IP address of LDAP server to add*>
Assigns a specific index number to the LDAP server you add. The index number you specify must be in use. LDAP servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves an LDAP server up or down in the list of configured servers. The index numbers you specify must be in use. To view all LDAP servers currently added to the system configuration, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /ldap/servernames LDAP Server names Menu

```
[LDAP servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert - Inserta new value
move - Move a value by number
```

The LDAP Servers menu enables you to list the configured LDAP servers, delete an LDAP server, or add a new LDAP server to the Portal configuration.

If you add more than one LDAP server to the list, remember that the first accessible LDAP server in the list will return a reply to the query. This stops the query, regardless of whether or not a match of the remote user's credentials were found. Therefore, the main purpose of adding more than one LDAP server is to provide for redundancy by ensuring that each listed LDAP server contains the same SSL VPN user database.

If your VPN users are dispersed in different LDAP server databases, you can configure another LDAP server using a different authentication ID. By including both authentication IDs in the authentication order, each LDAP server could then be used for authenticating different groups of users.

To enable LDAP authentication using the servers added to the list, make sure that the authentication ID that represents the LDAP configuration is included in the authentication order you have specified for the VPN. To view the current authentication order in the VPN, use the **/cfg/vpn <id>/aaa/authorder** command.

Table 69: LDAP server names Menu Options (/cfg/vpn/aaa/auth/ldap/servernames)

Command Syntax and Usage
list <*hostname*> <*port*> <*netbiosname*>
Displays all LDAP servers that are added to the LDAP configuration in the current VPN. The servers are listed by their host name, port, and netbios name.
del
Removes the specified LDAP server from the VPN configuration.
add <*hostname*> <*port*> <*netbiosname*>
Adds an LDAP server to the VPN. Specify the host name, port, and netbios name the LDAP server.

Command Syntax and Usage
Note: The default port number used by the LDAP protocol is 389. If LDAPS is enabled (using the **/cfg/vpn <id>/aaa/auth <id>/ldap/enaldaps** command) change the port number to 636.
insert <*position*> <*hostname*> <*port*> <*netbiosname*>
Assigns a specific index number to the LDAP server you add. Specify the index number, host name, port, and netbios name. The index number you specify must be in use. LDAP servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*value*> <*value*>
Moves an LDAP server up or down in the list of configured servers. The index numbers you specify must be in use.

/cfg/vpn <id> /aaa/auth <id> /ldap/ldapmacro LDAP Macro Configuration

```
[LDAP Macro Menu]

list       - List all values

del        - Delete a value by number

add        - Add a new value

insert     - Insert a new value  move - Move a value by number
```

The LDAP Macro menu 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.

Table 70: LDAP Macro Menu Options (/cfg/vpn/aaa/auth/ldap/ldapmacro)

Command Syntax and Usage
list Displays all LDAP macros that are added to the LDAP configuration in the current VPN. The macros are listed by their respective index number.
del <*LDAP macro by index number*> Removes the specified LDAP macro. Use the **list** command to display the index numbers of all added LDAP macros.
add <*variable name*> <*LDAP attribute*> <*prefix*> <*suffix*> Adds an LDAP macro to the configuration. • Variable name. The name of the variable, e.g. **exchangeServer**. By mapping the variable name to the LDAP attribute (see below), the corresponding value can be retrieved from the logged in user's LDAP/Active Directory user record. • LDAP attribute. Sets the LDAP user attribute whose value should be retrieved. • Prefix. Used 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. • Suffix. Used 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.
insert <*index number to insert at*> <*LDAP macro to add*> Assigns a specific index number to the LDAP macro you add. The index number you specify must be in use. LDAP macros with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*> Moves an LDAP macro up or down in the list of configured macros. The index numbers you specify must be in use. To view all LDAP macros currently added to the system configuration, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /ldap/groupsearc Group Search Configuration

```
[LDAP Group Search Menu]
```

```
groupbase       - Setgroup search base entry

memberattr      - Set LDAP groupmember attribute

ena             - Enable Group Search

dis             - Disable Group Search
```

The LDAP Group Search menu lets you configure the AVG to find group information on an iPlanet Directory Server.

Table 71: LDAP Group Search Menu Options (/cfg/vpn/aaa/auth/ldap/groupsearc)

Command Syntax and Usage
groupbase <*group searchbase entry*> 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 **/cfg/vpn <id>/aaa/auth <id>/enashortgr** setting (see Table 67: LDAP Menu Options (/cfg/vpn/aaa/auth/ldap) on page 180). Using the preceding example, the group name **Staff** would then be extracted from the group entry DN. The group should name should be defined in the VPN with one or more access rules (see the **/cfg/vpn <id>/aaa/group <id>** command on /cfg/vpn <id> /aaa/group <id> Group Configuration on page 226).
memberattr Defines the LDAP attribute that contains the group member's name. The default value is **uniqueMember.**
ena Enables the group search feature. Disabled by default.
dis Disables the group search feature. Disabled by default.

/cfg/vpn <id>/aaa/auth <id>/ldap/activedire Active Directory Settings Configuration

```
[Active Directory Menu]
enaexpiredaccount       Enable expired account/password check
expiredgroup            Set expired account group
exppasgroup             Set expired password group
pwdexppopup             Set Enable password expiration pop up warning
groupfromuserdn         Set Enable extraction of group from User DN
recursivemember         Enable recursive group membership
```

The Active Directory Settings menu lets you manage different Active Directory settings, for example expired account/password checks.

Table 72: Active Directory Settings Menu Options (/cfg/vpn/aaa/auth/ldap/activedire)

Command Syntax and Usage
enaexpiredaccount true|false Lets you specify the desired setting for expired account/password check. For passwords, the AVG computes (if possible) the number of days before the password will expire. This is displayed in a popup window for the user at Portal login when 5 days (or less) remains before the password expires. • **true:** The system will perform an account/password-expired check against Active Directory upon remote user login. • **false:** No account/password-expired check will be performed. The default value is **false.**
expiredgroup Sets the group in which users with expired accounts should be placed. Before using this command, define the user group in the Local database. As the only group link, configure a link to a site where the user can renew his/her account. Also remember to configure an access rule restricting access to the specified site.

Command Syntax and Usage
Group configuration is described on /cfg/vpn <id> /aaa/group <id> Group Configuration on page 226.
exppasgroup
Sets the group in which users with expired passwords should be placed. Before using this command, define the user group in the Local database. As the only group link, configure a link to a site where the user can change his/her password. Also remember to configure an access rule restricting access to the specified site. Group configuration is described on /cfg/vpn <id> /aaa/group <id> Group Configuration on page 226.
pwdexppopup true|false
Lets you turn off the popup warning. • **true:** A popup window is displayed to the user when 5 days (or less) remain before the password expires. • **false:** No popup warning is displayed. The default value is **true**.
groupfromuserdn true|false
Enables extraction group from the user domain after the password change. Active Directory is updated with the user domain group when you logon as a member of usergroup and submit the password. It returns the Distinguished Name only if the Active Directory does not return any groups. The default value is **false**.
recursivemember true|false
Lets you specify the desired setting for recursive group membership. • **true:** If the remote user belongs to an Active Directory group which, in its turn, belongs to another group, all groups are returned. • **false:** If the remote user belongs to an Active Directory group which, in its turn, belongs to another group, only the first group is returned. The default value is **false.**

/cfg/vpn <id> /aaa/auth <id> /ldap/adv Advanced LDAP Menu

```
[Advanced LDAP Menu]
enaxfilter      - Enable the extra search filter
xfilteratt      - Set LDAP extra search filter attribute
```

```
xfilterval      - Set LDAP extra search filter attribute value
```

The Advanced LDAP menu lets you configure the desired attribute/value when searching for a user record in an LDAP/Active Directory database. The feature is disabled by default, which means that no extra requirement is added when searching for a user record.

Table 73: Advanced LDAP Menu Options (/cfg/vpn/aaa/auth/ldap/adv)

Command Syntax and Usage
enaxfilter true|false Lets you enable the extra search filter. • **true**: The search filter is enabled. Continue with specifying the desired attribute/value using the commands below. • **false**: The search filter is disabled. The default value is **false**.
xfilteratt Sets the desired attribute when searching for user records. User records that contain this attribute and the value specified with the **xfilterval** command will be found. The default attribute is **objectclass**.
xfilterval Sets the desired value when searching for user records. User records that contain the attribute specified with the **xfilteratt** command and this value will be found. The default value is **person**.

/cfg/vpn <id> /auth <id> /ntlm NTLM Configuration

```
[NTLM Menu]

servers         - NTLM servers menu

exp             - Set password expired group
```

The NTLM menu is used for accessing the NTLM Servers menu, where the actual servers used for remote authentication of users can be specified. The menu also includes a command for placing remote users whose password has expired in a predefined group.

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 /cfg/vpn <id> /aaa/auth <id> /ntlm /servers NTLM Servers Menu on page 192).

To access the NTLM menu, the authentication type for the current authentication ID must be set to **ntlm**.

Table 74: NTLM Menu Options (/cfg/vpn/aaa/auth/ntlm)

Command Syntax and Usage
servers Displays the NTLM Servers menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /ntlm /servers NTLM Servers Menu on page 192.
exp *<group name>*
Sets the group in which the remote user should automatically be placed if the user's NTLM password has expired. Before using this command, define the user group in the Local database. Create a linkset with a link to a site where the user can change his NTLM password. Map the linkset to the group. Also remember to configure an access rule restricting access to the specified site. Group configuration is described on /cfg/vpn <id> /aaa/group <id> Group Configuration on page 226.

/cfg/vpn <id> /aaa/auth <id> /ntlm /servers NTLM Servers Menu

```
[NTLM servers Menu]

list        - List all values

del         - Delete a value by number

add         - Add a new value

insert      - Insert a new value

move        - Move a value by number
```

The NTLM Servers menu enables you to list the configured NTLM servers, delete an NTLM server, or add a new NTLM server to the VPN configuration.

To enable NTLM authentication using the servers added to the list, make sure that the authentication ID that represents the NTLM configuration is specified using the **/cfg/vpn <id> /aaa/authorder** command.

Table 75: Servers Menu Options (/cfg/vpn/aaa/auth/ntlm/servers)

Command Syntax and Usage
list Displays all NTLM servers that are added to the NTLM configuration in the current VPN. The servers are listed by their respective index number and IP address.
del *<NTLM server by index number>* Removes the specified NTLM server from the VPN configuration. Use the **list** command to display the index numbers of all added NTLM servers.
add *<IP address of NTLM server>* Adds an NTLM server to the VPN. Specify the IP address of the NTLM server. The next available index number is assigned automatically by the system. A maximum of three NTLM servers can co-exist in the configuration.
insert *<index number to insert at> <IP address of NTLM server to add>* Assigns a specific index number to the NTLM server you add. The index number you specify must be in use. NTLM servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move *<index number to move> <destination index number>* Moves an NTLM server up or down in the list of configured servers. The index numbers you specify must be in use. To view all NTLM servers currently added to the VPN configuration, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /siteminder SiteMinder Configuration

```
[SiteMinder Menu]

servers        - SiteMinder servers menu

fail over      - Set fail over mode

agent name     - Set SiteMinder agent name

secret         - Set SiteMinder shared secret
```

```
resource        - Set SiteMinder protected resource

groupattr       - Set SiteMinder group attribute

timeout         - Set SiteMinder server timeout

sso             - Allow SiteMinder Single-Sign for the VPN's domain

scope           - Set Domain Cookie scope

override        - Set Idle ttl override from Siteminder
```

The SiteMinder menu is used for configuring the current authentication ID to use a Netegrity SiteMinder authentication server. When the remote user logs in to the VPN using this authentication method, user name and password is checked against a SiteMinder server. Once the user is successfully authenticated, a user group is returned to the VPN Gateway from the SiteMinder server.

The VPN Gateway sets a SiteMinder 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 SiteMinder-aware backend server. The cookie is automatically validated against the SiteMinder policy server.

Note:

SiteMinder's tools for authorization are not supported. Access is granted based on the group access rules defined on the VPN Gateway. Challenge-based authentication replies (that is, the New PIN and Next Token modes of SecurID) from SiteMinder are not supported.

To access the SiteMinder menu, the authentication type for the current authentication ID must be set to siteminder.

Table 76: SiteMinder Menu Options (/cfg/vpn/aaa/auth/siteminder)

Command Syntax and Usage
servers Displays the SiteMinder Servers menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /siteminder/servers SiteMinder Servers Configuration on page 197.
failover failover|roundrobin If several SiteMinder authentication servers are configured, this setting defines the mode for accessing the servers.

Command Syntax and Usage
• Failover. If the SiteMinder server configured with index number 1 fails, the VPN Gateway will connect to the server configured with index number 2. • Round robin. The VPN Gateway will connect to the SiteMinder servers on a turn basis, that is, the first connection request is directed to the SiteMinder server configured with index number 1, the second to the server configured with index number 2 and so on. If only one SiteMinder server is configured, this setting has no effect. The default value is **roundrobin**.
agentname
Sets the name of the agent, that is, the VPN Gateway. The VPN Gateway will function as the client to SiteMinder. An agent with this exact name must be also configured in SiteMinder. For instructions on how to create an agent in SiteMinder, see the Technical Configuration Guide *Using Netegrity SiteMinder with Avaya VPN Gateway* available on http://www.avaya.com/support.
secret
Sets the secret used to authenticate the agent (that is, the VPN Gateway) to SiteMinder. The agent created in SiteMinder must have the same secret configured. For instructions on how to create an agent in SiteMinder, see the Technical Configuration Guide *Using Netegrity SiteMinder with Avaya VPN Gateway*.
resource
Sets the path to a protected resource that is also defined in SiteMinder. The default value is **GET:/**.
groupattr
Sets the group 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. For instructions on how to create an agent type in SiteMinder, see the Technical Configuration Guide *Using Netegrity SiteMinder with Avaya VPN Gateway* available on. The default value is **64**.
timeout
Sets a timeout value in seconds for a connection request to a SiteMinder server. If the timeout value elapses before a connection is established, authentication will fail. The default value is **5s** (5 seconds).
sso true|false
• **true**: Enables single sign-on. The VPN Gateway will automatically log in a remote user to the VPN if the user has a valid SMSESSION cookie from some

Command Syntax and Usage
other 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 the **wipecookie** command (see /cfg/vpn <id> /server/portal Portal Server Settings Configuration on page 266) is set to on (default value). If the remote user logs in to vpn.example.com without a valid SMSESSION cookie, the VPN Gateway will set the SMSESSION cookie as a domain cookie. This way the user can auto-log in to a.example.com . The SiteMinder session will however be invalidated if the user logs out from the Portal. • **false**: Single sign-on is disabled. **Note:** If **sso** is set to **true** but no display name or authentication order is configured for the SiteMinder authentication method on the VPN Gateway, it will not be possible to log in to the VPN without a valid SMSESSION cookie. Also see the **display** command on /cfg/vpn <id> /aaa/auth <id> Authentication Method Configuration on page 165 and the **authorder** command on /cfg/vpn <id> /aaa AAA Configuration on page 149. The default value is **false**.
scope <*integer*>
Determines the value of the domain cookie when **sso** (see above) is set to **true**. Example: • 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.
override <*override*>
Lets you override the timeout values returned by the siteminder server with the values configured in AVG.

/cfg/vpn <id> /aaa/auth <id> /siteminder/servers SiteMinder Servers Configuration

```
[SiteMinder servers Menu]

list            - List all values

del             - Delete a value by number

add             - Add a new value

insert          - Insert a new value

move            - Move a value by number
```

The SiteMinder servers menu enables you to list the configured SiteMinder servers, delete a SiteMinder server, or add a new SiteMinder server to the VPN configuration.

Table 77: SiteMinder Servers Menu Options (/cfg/vpn/aaa/auth/siteminder /server)

Command Syntax and Usage
list Displays all SiteMinder servers that are added to the SiteMinder configuration in the current VPN. The servers are listed by their respective index number and IP address.
del <*SiteMinder server by index number*>
Removes the specified SiteMinder server from the VPN configuration. Use the **list** command to display the index numbers of all added SiteMinder servers.
add <*IP address and port numbers of SiteMinder server*>
Adds a SiteMinder server with port numbers for authentication, authorization and accounting to the VPN configuration. Syntax example: add 10.10.10.10 44442 44443 44441 The next available index number is assigned automatically by the system. A maximum of three SiteMinder servers can co-exist in the configuration.
insert *<index number to insert at> <IP address of SiteMinder server to add>*
Assigns a specific index number to the SiteMinder server you add. The index number you specify must be in use. SiteMinder servers with an index number

Command Syntax and Usage
higher than (and including) the one you specify will have their current index number incremented by 1.
move *<index number to move> <destination index number>*
Moves a SiteMinder server up or down in the list of configured servers. The index numbers you specify must be in use. To view all SiteMinder servers currently added to the VPN, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /cleartrust ClearTrust Configuration

```
[ClearTrust Menu]

dispatcher      - ClearTrust dispatchers menu

servers         - ClearTrust authentication servers menu

distribute      - Set distributed mode

authtype        - Set authentication type

connection      - Set connection mode

timeout         - Set ClearTrust server timeout

sso             - Allow ClearTrust Single-Sign for the VPN's domain

scope           - Set Domain Cookie scope
```

Note:

The RSA SecurID New Pin mode is not supported when using Secondary Authentication service.

The ClearTrust menu is used for configuring the current authentication ID for use with an RSA ClearTrust authentication scheme. Besides installing the ClearTrust components (see the ClearTrust documentation) on the desired machines in your network, you should also configure the VPN Gateway to act as a ClearTrust web server agent and point out existing ClearTrust dispatcher(s) or authorization server(s).

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

on a ClearTrust-aware backend server. The cookie is automatically validated against the ClearTrust authorization server.

For instructions on how to configure client certificate authentication for a ClearTrust authentications scheme, see the **/cfg/vpn <id>/aaa/auth <id>/adv/validatedn** command on /cfg/vpn <id> /aaa/auth <id> /adv Advanced Settings Configuration on page 212.

To access the ClearTrust menu, the authentication type for the current authentication ID must be set to **cleartrust**.

Table 78: ClearTrust Menu Options (/cfg/vpn/aaa/auth/cleartrust)

Command Syntax and Usage
dispatcher Displays the ClearTrust dispatchers menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /cleartrust /dispatchers ClearTrust Dispatchers Configuration on page 201.
servers Displays the ClearTrust Servers menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /cleartrust /servers ClearTrust Servers Configuration on page 202.
distribute standard|distributed Sets the desired connection mode for the ClearTrust web server agent, that is, the VPN Gateway. • **standard**: The AVG sends requests to the first available ClearTrust authorization server in the list (see /cfg/vpn <id> /aaa/auth <id> /cleartrust /servers ClearTrust Servers Configuration on page 202). • **distributed**: The AVG distributes requests among all available ClearTrust authorization servers. It first chooses the server with the least number of outstanding packets. Where all servers are equal in outstanding packets, it picks the server with lowest average response time. Under low loads, a fraction of the requests are distributed randomly among eligible servers to keep the response time estimates updated and select faster servers. The default value is **distributed**.
authtype basic|nt|securid Sets the desired authentication type for the ClearTrust web server agent, that is, the VPN Gateway. • **basic**: Basic authentication validates the User ID and password provided at login with the user account information in the RSA ClearTrust data store. This is

Command Syntax and Usage
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 on how to enable SecurID authentication for a web server agent. The default value is **basic**.
connection clear|ssl_anon
Sets the desired connection type for the ClearTrust web server agent (the VPN Gateway) when connecting to other RSA ClearTrust components. • **clear**: Data sent between the ClearTrust components is not encrypted. • **ssl_anon**: Data sent between the ClearTrust components is encrypted using anonymous SSL, that is, neither the client nor the server is required to present a certificate to authenticate itself. A tunnel is set up between communicating servers, using 128-bit encryption. When this option is selected, all the RSA ClearTrust components (the ClearTrust Servers and Agents) must be configured to use anonymous SSL. The default value is **ssl_anon**.
timeout <*seconds*>
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 **5s** (5 seconds).
sso true|false
• **true**: Enables single sign-on. The VPN Gateway will 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 the **wipecookie** command (see /cfg/vpn <id> /server/portal Portal Server Settings Configuration on page 266) is set to on (default value). If the remote user logs in to vpn.example.com without a valid CTSESSION cookie, the VPN Gateway will set the CTSESSION cookie as a domain cookie.

Command Syntax and Usage
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. • **false**: Single sign-on is disabled. **Note:** If sso is set to true but no display name or authentication order is configured for the ClearTrust authentication method on the VPN Gateway, it will not be possible to log in to the VPN without a valid CTSESSION cookie. Also see the **display** command on /cfg/vpn <id> /aaa/auth <id> Authentication Method Configuration on page 165 and the **authorder** command on /cfg/vpn <id> /aaa AAA Configuration on page 149. The default value is **false**.
scope <*integer*>
Determines the value of the domain cookie when **sso** (see above) is set to **true**. Example: • 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.

/cfg/vpn <id> /aaa/auth <id> /cleartrust /dispatchers ClearTrust Dispatchers Configuration

```
[ClearTrust dispatchers Menu]
list       - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The ClearTrust dispatchers menu lets you point out one or several dispatchers that have previously been installed in the RSA ClearTrust setup. 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 in the event of a failure. See the ClearTrust documentation for more information about the dispatcher component.

Table 79: ClearTrust Dispatchers Menu Options (/cfg/vpn/aaa/auth/cleartrust / dispatchers)

Command Syntax and Usage
list Lists all dispatchers that have been added to the ClearTrust configuration in the current VPN. The dispatchers are listed by index number.
del *<dispatcher by index number>* Removes the specified dispatcher from the VPN configuration. Use the **list** command to display the index numbers of all added dispatchers.
add *<host name> <port number>* Adds a dispatcher with port number to the configuration. Syntax example: **add www.example.com 5608** The next available index number is assigned automatically by the system.
insert *<index number to insert at> <host name and port number of dispatcher to add>* Assigns a specific index number to the dispatcher you add. The index number you specify must be in use. Dispatchers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move *<index number to move> <destination index number>* Moves a dispatcher up or down in the list of configured dispatchers. The index numbers you specify must be in use. To view all dispatchers currently added to the VPN, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /cleartrust /servers ClearTrust Servers Configuration

```
[ClearTrust servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

Instead of letting the dispatcher (see /cfg/vpn <id> /aaa/auth <id> /cleartrust /dispatchers ClearTrust Dispatchers Configuration on page 201) manage communication with the ClearTrust authorization server(s) you can have the web server agent (that is, the AVG) communicate directly with the authorization server(s). The ClearTrust servers menu lets you

list configured RSA ClearTrust authorization servers, delete a server, or add a new server to the configuration. Note that if a dispatcher is configured on the AVG, any authorization servers configured on the AVG will be ignored.

Table 80: ClearTrust Servers Menu Options (/cfg/vpn/aaa/auth/cleartrust /servers)

Command Syntax and Usage
list Lists all ClearTrust authorization servers that have been added to the configuration in the current VPN. The servers are listed by their respective index number and host name.
del <*ClearTrust server by index number*> Removes the specified server from the configuration. Use the **list** command to display the index numbers of all added ClearTrust authorization servers.
add <*host name*> <*port number*> Adds a ClearTrust authorization server (with port number) to the VPN configuration. Syntax example: add **www.example.com 5615** The next available index number is assigned automatically by the system.
insert <*index number to insert at*> <*host name of ClearTrust server to add*> Assigns a specific index number to the ClearTrust server you add. The index number you specify must be in use. ClearTrust servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*> Moves a ClearTrust server up or down in the list of configured servers. The index numbers you specify must be in use. To view all ClearTrust servers currently added to the VPN, use the **list** command.

/cfg/vpn <id> /aaa/auth <id> /rsa RSA SecurID Configuration

```
[RSA Menu]
rsaname    - Set RSA server symbolic name
rsagroup   - Set group for RSA authenticated users
```

The RSA menu is used for configuring remote user authentication of users by way of RSA SecurID. To authenticate to the RSA server, the remote user generates a single-use password from his or her RSA SecurID token. Apart from configuring the RSA authentication method from this menu, the RSA server specifics should be configured (see /cfg/sys/rsa RSA Server Configuration on page 424).

Note:

The RSA SecureID New Pin Mode is not supported as Secondary authentication.

To access the RSA menu, the authentication type for the current authentication ID must be set to `rsa` .

Table 81: RSA Menu Options (/cfg/vpn/aaa/auth/rsa)

Command Syntax and Usage
rsaname References the symbolic name given to the RSA server using the **/cfg/sys/rsa** command (see /cfg/sys/rsa RSA Server Configuration on page 424).
rsagroup Sets the user access group (as defined on the VPN Gateway) to which authenticated users will be assigned. The access rules pertaining to this group will determine the user's access rights.

/cfg/vpn <id> /aaa/auth <id> /local Local Database Configuration

```
[Local database Menu]
add  - Add/edit user in local database
passwd     - Change user's password in local database
pwdage     - Set Change user's password age
expirewarn - Set Password expire warning interval
pwdtext    - Set Message on passwd policy
groups     - Change user's groups in local database
del  - Delete user from local database
list - List users in local database
import     - Import database from TFTP/FTP/SCP/SFTP server
export     - Export database to TFTP/FTP/SCP/SFTP server
```

The Local database menu is used for managing user authentication locally, where users are added to a database in the AVG cluster. Local database authentication can be used in parallel with external database authentication (for example RADIUS, LDAP or NTLM). Configuring the VPN Gateway to use local database authentication is mainly useful in the following scenarios:

- Quickly adding a limited number of VPN users.
- Providing a group of users, such as a project group for example, access to the VPN for a limited time.
- For testing purposes.

Table 82: Local database Menu Options (/cfg/vpn/aaa/auth/local)

Command Syntax and Usage
add *<user name> <password> <group name(s)>* Adds a user to the local authentication database. You need to provide the user name and password for the user, as well as the group(s) in which the user is a member. The user name must be unique. When the user attempts to log in to the VPN and local database authentication is applied, the user is prompted for the user name and password you define here. The group name is used for authorization, controlling access to resources by checking the specified group name against one or more access rules associated with the group. The group name you specify when adding a user must therefore exist in the current VPN, along with one or more access rules valid for the group. To view which group names and associated access rules that are currently defined in the VPN, use the **/cfg/vpn <id>/aaa/cur group** command. **Note:** If a user is authenticated by an external authentication server (for example RADIUS or LDAP), and that server cannot be configured to return a list of group names upon authentication, the local database can be used for authorization only. To achieve such a "division of labor", provide the user name and group name(s) when prompted, but substitute the actual password for the specified user name with an asterisk (*). Example from CLI session: `>> Local database# add Enter user name: john Enter passwd: [press enter to leave unchanged] * Enter group names (comma separated) :staff` For instructions on how to configure the VPN Gateway to perform external database authentication in conjunction with local database authorization, see the groupauth command on Table 90: Advanced Settings Menu Options (/cfg/vpn/aaa/auth/adv) on page 213.
passwd *<user> <new password>*
Lets you change the password for an existing user.
pwdage *<integer>*
Lets you set the age of password for an existing user.
expirewarn *<integer>*
Lets you set the time interval for post warning when the password is due to expire for an existing user.
pwdtext *<string>*
Lets you set a message on password policy.
groups *<user> <desired group names>*
Lets you change the groups list for an existing user.
del *<user by name>*

Command Syntax and Usage
Deletes the specified user from the local user database.
list
Lists all users added to the local database by user name, password (encrypted), and group membership. The maximum number of entries in the database that can be displayed simultaneously using the list command is 1000. If there are more than 1000 entries in the database, you can narrow your search by modifying the **list** command using a string of characters directly followed by an asterisk (*). Example: The command **list jo*** displays all entries with user names starting with jo .
import *<protocol [tftp|ftp|scp|sftp]> <server host name or IP address> <file name> <key for user password protection> <FTP server user name and password>*
Imports a populated database from a TFTP/FTP/SCP/SFTP server. 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.
export *<protocol [tftp|ftp|scp|sftp]> <server host name or IP address> <destination file name> <key for user password protection> <FTP server user name and password>*
Exports the local database as a file (e.g. db.txt) in ASCII format to a TFTP/FTP/SCP/SFTP server. Below is an example of an exported user record with the password encrypted: **john:$2$7á?yLs...ßìöonž±†:trusted** where **2** indicates an encrypted password

/cfg/vpn <id>/aaa/auth <id>/http HTTP authentication

```
[HTTP Menu]
      serverip   - Set HTTP server address
      port       - Set HTTP server port
      type       - Set authentication type
      path       - Set directory path on the http server
      secure     - Set secure https mode
      httpgroup  - Set Group for HTTP authenticated users
      httpdomain - Set Domain for HTTP authenticated users
```

The HTTP menu is used for configuring HTTP authentication. The HTTP authentication can be used for portal, IPsec, and Net Direct logon.

The WWW-Authenticate handshake takes place resulting in the validation of credentials. If authentication is not enabled on the back-end HTTP server, the validation fails and the access is rejected.

Table 83: HTTP Menu Options (/cfg/vpn/aaa/auth/http)

Command Syntax and Usage
serverip <string> Lets you set HTTP server address.
port <string> Lets you set HTTP server port.
type <basic|digest|ntlm> Lets you set HTTP authentication type.
path <string> Lets you set directory path on the HTTP server.
secure <true|false> Lets you enable or disable secure https mode.
httpgroup <string> Lets you set group for HTTP authenticated users.
httpdomain <string> Lets you set domain for HTTP authenticated users.

/cfg/vpn <id>/aaa/auth <id>/cert Client Certificate Authentication

```
[Cert Menu]
cacerts     - CACerts menu
groupoids   - Group OIDs menu
useroid     - User OID menu
```

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

Values in the client certificate's subject part, identified as user OID and group OID, will be extracted to authenticate the remote user to the VPN Gateway and assign one or several group names to the user. No password is required, which means that single sign-on to backend servers will not be possible.

As an alternative or complement, group names can be mapped to the CA certificate used to generate the client certificate. See the **cacerts** command below.

Note:

The Portal will accept client certificates for authentication provided that only one authentication ID of the `cert` type has been configured and enabled.

For a full example on how to configure client certificate authentication, see the "Authentication Methods" chapter in the *Application Guide for VPN*.

Table 84: Cert Menu Options (/cfg/vpn/aaa/auth/cert)

Command Syntax and Usage
cacerts Displays the CACerts menu. To view menu options, see /cfg/vpn <id> /aaa/auth <id> /cert/cacerts CACerts Groups Configuration on page 209.
groupoids Displays the Group OIDs menu. To view menu options, see /cfg/vpn <id> /aaa/ auth <id> /cert /groupoids Group OIDs Configuration on page 209.
useroid Displays the UserOID Menu. For more information about options, see /cfg/vpn <id>/aaa/auth <id>/cert/useroid User OID Configuration on page 210.

/cfg/vpn <id> /aaa/auth <id> /cert/cacerts CACerts Groups Configuration

```
[CACerts Menu]
list - List all values
del  - Delete a value by number
add        - Add a new value
```

The CACerts menu can be used as another (or additional) method of assigning user groups to a user. The only thing you have to do is map existing AVG group names to specific CA certificates. If the remote user authenticates to the VPN Gateway with a client certificate signed with a CA certificate listed here, the corresponding group name is assigned to that user.

This method can be combined with the group OIDs method (see the next page).

Table 85: CACerts Menu Options (/cfg/vpn/aaa/auth/cert/cacerts)

Command Syntax and Usage
list Lists configured CA certificates and the groups that are assigned to each CA certificate.
del
Deletes the desired entry by index number. Use the **list** command to view the index numbers.
add
Adds a new entry to the list. Start by entering the desired CA certificate number. Press TAB to view existing numbers. Then map the desired group name to the CA certificate. You can only map one group to the CA certificate. Press TAB to view existing group names. Keep in mind that group names are case sensitive.

/cfg/vpn <id> /aaa/auth <id> /cert /groupoids Group OIDs Configuration

```
[GroupOIDs Menu]
list - List all values
```

```
del  - Delete a value by number
add  - Add a new value
```

The GroupOIDs menu is used for specifying which of the OIDs (object identifiers) in the client certificate's subject part that should be used to identify group names. As opposed to user name, several group names can be extracted from the client certificate.

Table 86: GroupOIDS Menu Options (/cfg/vpn/aaa/auth/cert/groupoids)

Command Syntax and Usage
list Lists configured group OIDs.
del Deletes the desired entry by index number. Use the **list** command to view the index numbers.
add *<numeric OID, e.g. 2.5.4.7>* Lets you add an OID (object identifier) from the subject part of the client certificate. The value that corresponds to this OID will be extracted from the certificate and used as group name when the remote user connects to the Portal. One or several OIDs in the client certificate can be specified as **groupoid** . The group name specified as the value in the client certificate must correspond to an existing group name configured on the VPN Gateway. Enter the appropriate numeric OID when prompted: Example: `Enter group OID within 'subject' :` **2.5.4.7** To view available OIDs and values for an existing certificate, use the **/cfg/cert #/subject** command. Example from the output: `L/localityName (2.5.4.7) = groupname` where localityName is the symbolic name, 2.5.4.7 is the OID and groupname is the value. For information about how to generate a new client certificate and export it to a file, see the "Certificates and Client Authentication" chapter in the *User's Guide*.

/cfg/vpn <id>/aaa/auth <id>/cert/useroid User OID Configuration

```
[UserOID Menu]
subject    - Subject menu
subalt  -  Subject alternative menu
```

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 do not need any special manipulation to use the CAC support as subject alternate name supports Microsoft UPN in client certificate.

Table 87: User OID Menu options (/cfg/vpn/aaa/auth/cert/useroid)

Command Syntax and Usage
subname Displays the Subject Menu. For more information about options, see /cfg/vpn <id>/aaa/auth <id>/cert/useroid/subject Subject Menu on page 211.
subalt Displays the SubAlt Menu. For more information about options, see /cfg/vpn <id>/aaa/auth <id>/cert/useroid/subalt Subject Alternate Menu on page 212.

/cfg/vpn <id>/aaa/auth <id>/cert/useroid/subject Subject Menu

```
[Subject Menu]
name    - Set subject name
suffix  - Set suffix
```

Use the Subject Menu to specify the subject name in the client certificate.

Table 88: Subject Menu options (/cfg/vpn/aaa/auth/cert/useroid/subname)

Command Syntax and Usage
name Lets you extract the user from general names inside the subject name. Valid values for general names are commonName, emailAddress, givenName, initials, surname, and title.
suffix The option appears when CAC is enabled in the Advanced menu. To enable CAC, enter command **cfg/vpn <id>/aaa/auth <id>/adv/cac/ena**. For more information, see /cfg/vpn <id>/aaa/auth/adv/cac Common Access Card Menu on page 215. To support CAC for US Department of Defense, use this option to append the configured string to the subject name. The suffix string blindly appends to any type of subject name. For CAC support, it must be used with commonName type. Valid string value is up to 255 characters.

/cfg/vpn <id>/aaa/auth <id>/cert/useroid/subalt Subject Alternate Menu

```
[SubAlt Menu]
name    - Set general name
ena    - Enable subject alternative
dis   - Disable subject alternative
```

Use the SubAlt Menu to specify the type of the name in the client certificate.

Table 89: Subject Alternate Menu options (/cfg/vpn/aaa/auth/cert/useroid/subalt)

Command Syntax and Usage
name
Displays the current subject value. In the client certificate you can specify the type of the name in the subject alternative name. The supported types are otherName. The otherName type is specific to the Microsoft UPN support.
ena
Enables the subject alternate name. The subject alternate name overrides subject name when the subalt option is enabled. Disable the CAC option to use subalt option. For more information about CAC, see /cfg/vpn <id>/aaa/auth/adv/cac Common Access Card Menu on page 215.
dis
Disables the subject alternate name.

/cfg/vpn <id> /aaa/auth <id> /adv Advanced Settings Configuration

```
[Advanced Menu]

group auth          - Set Authentication server list for group information

second auth         - Set Secondary authentication server

validate dn         - Set Validate Cert-DNby Clear trust server
```

revcert dn	- Reverse Cert-DN before Cleartrust validation
cac	CAC support menu

The Advanced Settings menu includes commands for configuring the current authentication method to retrieve user group information from other authentication schemes besides the current one and for configuring a second authentication server.

Table 90: Advanced Settings Menu Options (/cfg/vpn/aaa/auth/adv)

Command Syntax and Usage
groupauth <*authentication method ID(s), separated by comma*> By referencing a previously defined authentication ID here, the system will retrieve the remote user's group information from the corresponding authentication scheme. If LDAP variables have been configured, these will also be retrieved. Example: The user logs in through RADIUS but the user groups are stored in an LDAP database. By entering a list of authentication IDs separated by comma (for example 1,3,2), the system will check 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 remote user's login session. **Note:** Group information (and variables) can only be retrieved from the Local database and LDAP databases. If user groups exist in the current authentication scheme, these will be added to the user groups found in the referenced authentication scheme(s). For instructions on how to add users to the Local database for authorization only, that is, when authentication is performed by a remote server, see the **add** command on Table 82: Local database Menu Options (/cfg/vpn/aaa/auth/local) on page 205.
secondauth <*authentication method ID*> Lets you specify a second authentication method to be used after the first one succeeds. The secondauth command supports single-sign on to backend servers when the first authentication method is token-based or uses client certificate authentication. Groups retrieved from the second authentication server (if any) are added to the groups retrieved from the current authentication scheme (like the **groupauth** command above). Release 9.0 supports IPsec Two Factor authentication. 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. If a second authentication method is specified, an extra password field is added to the Portal login page. To enable CAC support, enable the second authentication

Command Syntax and Usage
menu with LDAP support. The LDAP authentication must be configured to support Microsoft UPN. For more information about LDAP, see Table 67: LDAP Menu Options (/cfg/vpn/aaa/auth/ldap) on page 180. This command is only available if the authentication method is set to **radius**, **cert** or **rsa**.
validatedn <*ClearTrust authentication method ID*>
This command is only available if the current authentication method is set to **cert**. Lets you reference an authentication ID representing a ClearTrust authentication scheme. By binding a Client certificate authentication ID to a ClearTrust authentication ID, the user can authenticate to the ClearTrust server using a client certificate. The client certificate's subject DN string is matched against the corresponding string specified in the user record of the RSA ClearTrust authorization server. The string extracted from the user's client certificate is exemplified below: `c=US,st=Colorado,l=Denver,o=Company,ou=Accounting,cn=John` This string should be specified as the client certificate DN for the user record in the ClearTrust authorization server.
revcertdn true|false
Lets you reverse the order of the DN string components for compatibility with the ClearTrust Web Agent configuration parameter cleartrust.agent.reverse_certificate_dn. If the latter setting is "True", the **revcertdn** command must also be set to **true**. • **true**: Reverses the certificate DN string before sending it to the ClearTrust authorization server for validation. Using the string in the preceding example (see the **validatedn** command) the string sent would be: cn=John,ou=Accounting,o=Company,l=Denver,st=Colorado,c=US • **false**: The string is not reversed, that is, it will look like in the example in above (see the **validatedn** command). The default value is **false**.
cac
Displays the CAC Menu. For more information about options, see /cfg/vpn <id>/aaa/auth/adv/cac Common Access Card Menu on page 215.

/cfg/vpn <id>/aaa/auth/seqauth Sequential Authentication Menu

```
[SeqAuth Menu]
      ena         - Enable Sequential Authentication
      dis         - Disable Sequential Authentication
      copyuser    - Set Enforce same username for second auth
      usesecond   - Set Use secondary credentials for SSO and Iauto
      retries     - Set Number of retries for secondary login
```

Use the SeqAuth Menu to configure sequential authorization.

Table 91: Sequential Authentication Menu options (/cfg/vpn <id>/aaa/auth/seqauth)

Command Syntax and Usage
ena Enables sequential authentication.
dis Disables sequential authentication.
copyuser on|off Lets you use the same user name for the secondary authentication.
usesecond on|off Lets you use the secondary credentials for Single Sign-On (SSO) and i-auto.
retries <1-3> Lets you specify the number of retries. The number of retries can be between 1 and 3.

/cfg/vpn <id>/aaa/auth/adv/cac Common Access Card Menu

```
CAC Menu

ena   -enable CAC support

dis   -disable CAC support
```

Use the CAC Menu to enable or disable the Common Access Card (CAC) support for the certificate authentication.

Table 92: CAC Menu options (/cfg/vpn/aaa/auth/adv/cac)

Command Syntax and Usage
ena
Enables the U.S. Department of Defense CAC support. Subject name in the client certificate is extracted and manipulated to meet DoD CAC support requirement. You must disable subject alternate name to enable CAC. For more information, see /cfg/vpn <id>/aaa/auth <id>/cert/useroid/subalt Subject Alternate Menu on page 212.
dis
Disables CAC support for the certificate authentication.

/cfg/vpn <id> /aaa/network <id> Network Access Configuration

```
[Network 1 Menu]
name - Set network name
subnet     - Subnet menu
comment    - Set comment
del  - Remove network
```

The Network menu is 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 or reject access to the network.

When a remote user requests a resource over the Internet, the user's group membership and access rules will determine which networks the user is authorized to.

See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of groups, access rules and profiles.

Table 93: Network Menu Options (/cfg/vpn/aaa/network)

Command Syntax and Usage
name
Assigns a name to the current network. This name can later be referenced in one of the access rules for a specific user group, using the **/cfg/vpn <id>/aaa/group <id>/access #/network** command. A network definition can also be referenced in a client filter to shape the access rights to intranet resources according to the remote user's source network or IP address. To reference the network definition in a client filter, use the **/cfg/vpn <id>/aaa/filter #/clientnet** command.

Command Syntax and Usage
subnet
Displays the Subnet menu where several subnet entries (each defining a network address and netmask) can be configured. To view menu options, see /cfg/vpn <id> /aaa/network <id > /subnet <id> Subnet Access Configuration on page 217.
comment
Lets you enter a comment for the current network definition, for example a text explaining which network segment(s) the entry refers to.
del
Removes the network definition from the current configuration.

/cfg/vpn <id> /aaa/network <id > /subnet <id> Subnet Access Configuration

```
[Network Subnet 1 Menu]
host - Set Host Name
net  - Set network address
mask - Set network mask
del  - Remove subnet
```

The Subnet menu is used to configure an optional number of subnet entries, each defining hosts, networks or network ranges to be included in the current network definition.

Table 94: Subnet Menu Options (/cfg/vpn/aaa/network/subnet)

Command Syntax and Usage
host *<host name>*
Sets a specific host, or all hosts within a subdomain or second level domain. The host name can be specified as a fully qualified domain name (FQDN) to target a specific host. To specify all hosts within a second level domain or subdomain, you can use an asterisk (*) as a wildcard. Example: *.secondleveldomain.topleveldomain Or *.subdomain.secondleveldomain.topleveldomain **Note:** You can use either the **host** command to specify a host (or a range of hosts using an asterisk), or a combination of network address and subnet mask (using the net and mask commands). If you specify hosts using both the host command and the net/mask commands, you will receive an error message in the CLI when applying the changes.

Command Syntax and Usage
Note: Hosts specified with this command will be ignored for IPsec and Net Direct. Use the net and mask commands (see below) instead.
net <*network address*>
Defines the hosts that together with the subnet mask (see below) make up one of the subnet definitions for the current network. The default net address is set to 0.0.0.0.
mask <*network mask*>
Sets the subnet mask for the network address, limiting the validity to a specific host or range of hosts. The other settings in the access rule thereby only apply to the specified range. The default subnet mask is set to 255.255.255.255. Combined with the default network address of 0.0.0.0, the default subnet mask mean that no hosts can be accessed. Note that the subnet mask can be entered in number of bits, for example 32 instead of 255.255.255.255.
del
Removes the subnet from the current network definition.

/cfg/vpn <id> /aaa/service <id> Service Access Configuration

```
[Service 1 Menu]
name - Set service name
protocol   - Set allowed protocols
ports- Set allowed port
comment    - Set comment
del  - Remove Service
```

The Service menu is used to specify the services (ports and protocols) to which members of a specific user group should be authorized when requesting a resource. The name of the service (as specified using the **name** command) can later be referenced to make up one of the access rules for a specific user group.

See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of groups, access rules and profiles.

Table 95: Service Menu Options (/cfg/vpn/aaa/service)

Command Syntax and Usage
name

Command Syntax and Usage
Assigns a name to the current service definition. This name should be referenced when configuring the access rules for a specific user group, using the **/cfg/vpn <id>/aaa/group <id>/access <id>/service** command. When running the AAA Quick Setup wizard, the following service definitions will be created: • http. Uses TCP port 80. • https. Uses TCP port 443. • web. Uses TCP ports 20, 21, 80 and 443. • smtp. Uses TCP port 25. • pop3. Uses TCP port 110. • imap. Uses TCP port 143. • email. Uses TCP ports 25, 110 and 443. • telnet. Uses TCP port 23. • ssh. Uses TCP port 22. • ftp. Uses TCP ports 20 and 21. • smb. Uses TCP port 139. • fileshare. Uses TCP ports 20, 21 and 139.
protocol *<protocols, separated by comma (,)>*
Sets the allowed protocols for the configured ports. Available protocols are TCP and UDP. To allow several protocols, enter the desired protocols separated by comma.
ports *<port numbers, separated by comma (,)>*
Sets the allowed port numbers for the current service definition. You can specify single port numbers (separated by comma) or a range of port numbers, or both. Example: 80,443 Or 25,80,443,1000-2000 Or 0 (meaning all ports)
comment
Lets you enter a comment for the current service, for example a text explaining which services the current service definition refers to.
del
Removes the service from the current configuration.

/cfg/vpn <id> /aaa/appspec <id> Application Specific Menu

```
[AppSpecific 1 Menu]
name - Set appspec name
path - Set path
comment    - Set comment
del  - Remove AppSpec
```

The Appspec menu is used to specify a path to an intranet resource, for example to a specific folder on an FTP file server. The name of the appspec entry (as specified using the **name** command) can later be referenced to make up one of the access rules for a specific user group.

The appspec definition identifies a path, for example **/public**. Combined with a host identified by a network reference in the same access rule, the group members can be granted (or denied) access to a subfolder on that host.

See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of groups, access rules and profiles.

Table 96: Appspec Menu Options (/cfg/vpn/aaa/appspec)

Command Syntax and Usage
name Assigns a name to the current appspec entry. This name should be referenced when configuring the access rules for a specific user group, using the **/cfg/vpn <id>/aaa/group <id>/access <id>/appspec** command.
path Defines the path to a subfolder on the host(s) identified by the network reference selected for the current access rule. The path denotes the part of the URL that follows the IP address of hosts included in the network reference. Example: Suppose the IP address (for example 192.168.128.10) specified as one of the subnets in a network definition identifies a web server with the domain name www.example.com. By specifying /public as the path, a remote user who tries to access the following URL will create a match: www.example.com/public. The default setting is blank, which means that any path is valid in the specified domain. 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 below:

Command Syntax and Usage
• 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.
comment
Lets you enter a comment for the current appspec entry, for example a text explaining which paths the current appspec entry refers to.
del
Removes the appspec entry from the current configuration.

/cfg/vpn <id>/aaa/extspec <1-1023> File Extension Specifications Menu

```
[FileExtSpec 1 Menu]
      name       - Set extspec name
      extensions - Extensions menu
      comment    - Set comment
      del        - Remove FileExtension
```

Table 97: File Extension Specifications Menu Options (/cfg/vpn/aaa/extspec)

Command Syntax and Usage
name
Lets you specify file extension list name.
extensions
Displays the Extensions Menu. For more information about options, see /cfg/vpn <id>/aaa/extspec <1-1023>/extensions Extensions Menu on page 222.
comment
Lets you provide a description for the file extension list.
del
The file extension specification is deleted when the changes are applied.

/cfg/vpn <id>/aaa/extspec <1-1023>/extensions Extensions Menu

```
[Extensions Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

Table 98: File Extension Specifications Menu Options (/cfg/vpn <id>/aaa/extspec)

Command Syntax and Usage
list Lists all values in the File Extensions specification list.
del <index number> Deletes the file from the specified index number.
add <index number> Adds files in the specified index number.
insert <index number> Inserts the files in the specified index number.
move <index to move> <destination index> Moves the file from a specified index number to another index number.

/cfg/vpn <id> /aaa/filter <id> Client Filter Configuration

```
[Client Filter 1 Menu]
      name       - Set filter name
      cert       - Client certificate present
      iewiper    - IE cache wiper present
      tg         - TunnelGuard checks passed
      nap        - NAP checks passed
      methods    - Set access methods
      authserver - Set authentication servers
      clientnet  - Set client network reference
      comment    - Set comment
      del        - Remove client filter
```

The Client Filter menu includes different client filter types, each defining a security aspect related to the remote user's connection, for example how the user was authenticated (**authserver**) or from which network the connection originated (**clientnet**).

If the connection is considered secure, more generous access rights can be granted to the user. These access rights should be specified in an extended profile for the specific user group.

The extended profile is triggered when there is a match between the client filter (referenced in the extended profile) and the user's connection specifics.

For examples on how to apply client filters and extended profiles, see the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* .

Table 99: Client Filter Menu Options (/cfg/vpn/aaa/filter)

Command Syntax and Usage
name Assigns a name to the current client filter. This name should later be referenced in a user group's extended profile, using the **/cfg/vpn <id>/aaa/group <id>/extend <id>/filter** command.
cert true|false|ignore This command can be used if you wish to create an extended profile with more generous access rights for remote users with a client certificate installed. • **true:** The client filter triggers when the remote user authenticates with a client certificate. To grant this user more generous access rights, create an extended profile, reference the client filter you have just created and specify the desired access rules. • **false:** The client filter triggers when the remote user does not authenticate with a client certificate. To give this user limited access rights, create an extended profile, reference the client filter you have just created and specify the desired access rules. • **ignore:** The client filter will not be triggered by the presence or absence of a client certificate. The default value is **ignore**.
iewiper true|false|ignore This command can be used if you wish to create an extended profile with more generous access rules for remote users who have installed the IE cache wiper on their local machines. Upon Portal login, the user is offered to download the IE cache wiper (if enabled). • **true:** The client filter triggers when the IE cache wiper is detected on the remote user's machine. To grant this user more generous access rights, create an extended profile, reference the client filter you have just created and specify the desired access rules. • **false:** The client filter triggers when no IE cache wiper is detected on the remote user's machine. To give this user limited access rights, create an extended profile, reference the client filter you have just created and specify the desired access rules. • **ignore:** The client filter will not be triggered by the presence or absence of the IE cache wiper. The default value is **ignore**.

Command Syntax and Usage
tg true|false|ignore
This command can be used if you wish to create an extended profile with more generous access rules for remote users whose computers have passed an integrity check made by Tunnel Guard. With Tunnel Guard enabled, the Tunnel Guard applet is downloaded to the client machine and activated once the client is logged in to the VPN. Tunnel Guard checks the client machine for the required components and notifies the VPN Gateway whether the check has succeeded or failed. For instructions on how to configure Tunnel Guard, see the "Configure Tunnel Guard" chapter in the *Application Guide for VPN* . • **true:** The client filter triggers when the Tunnel Guard checks have succeeded. To grant this user more generous access rights, create an extended profile, reference the client filter you have just created and specify the desired access rules. • **false:** The client filter triggers the Tunnel Guard checks have failed. To give this user limited access rights, create an extended profile, reference the client filter you have just created and specify the desired access rules. • **ignore:** The client filter will not be triggered, irrespective of the result of a possible Tunnel Guard check. The default value is **ignore**.
nap
Lets you view and set the NAP filter. Based on the result, you can configure the extended profiles. The default NAP filter value is **ignore**. The NAP filter values are as follows: • **true**: The client filter triggers when the NAP check is successful. To grant this user more generous access rights, create an extended profile, reference the created client filter and specify the desired access rules. • **false**: The client filter triggers when the NAP check is a failure. To give this user limited access rights, create an extended profile, reference the created client filter and specify the desired access rules. • **unsupported**: The client filter is triggered when the client machine is not NAP aware. • **ignore**: The client filter is not triggered and this is irrespective of the NAP check result.
methods *<access methods separated by comma (,)>*
Defines the access method(s) by which a user authenticates/requests resources over the Internet. The following methods are available:

Command Syntax and Usage
• **ssl.** The remote user authenticates to the VPN and sets up an SSL session, either through the browser (clientless mode) or through the installed SSL VPN client (transparent mode). • **ipsec.** The user authenticates to the VPN and sets up an IPsec tunnel using the IPsec VPN client (formerly Contivity). • **netdirect.** The user authenticates to the VPN through the browser and sets up an SSL session using the Net Direct client. The Net Direct client is downloaded to the remote user's machine for full access to the intranet (that is, not through the Portal). • **SPO.** The user authenticates to the VPN through SPO client.
authserver <*authentication server names, separated by comma (,)*>
Specifies which authentication server or servers are used for client authentication. To view available authentication servers, press TAB following the **authserver** command. Example: Token authentication is considered more secure. The access rights specified for an extended profile whose client filter identifies an authentication server for token authentication could be more generous.
clientnet
Lets you reference a previously created network definition identifying a client network. To create a network definition, use the **/cfg/vpn <id>/aaa/network** command. Example: A branch office network is considered more secure. The access rights specified for an extended profile whose client filter identifies a branch office network could be more generous. If the connects to the VPN from the branch office network, the extended profile is triggered. If the user connects to the VPN from an Internet café, no match is found between the user's source network and the network referenced in the client filter. Only the base profile's access rules are applied.
comment
Lets you enter a comment for the current client filter.
del
Removes the client filter from the current configuration.

/cfg/vpn <id> /aaa/group <id> Group Configuration

```
[Group 1 Menu]
      name       - Set group name
      access     - Access rule menu
      spoaccess  - Set SPO Client feature access
      sposwindex - SPO Application index menu
      print      - Print access rules
      restrict   - Set number of login sessions
      usertype   - Set portal user type
      idlettl    - Set login session idle time
      sessionttl - Set maximum session length
      ndwauser   - Set Netdirect windows admin user name
      ndwapasswo - Set Netdirect windows admin password
      linkset    - Linkset menu
      extend     - Extended profiles menu
      tgsrs      - Set TunnelGuard SRS Rule
      ippool     - Set IP pool
      hippool    - Set Host IP pool
      l2tp       - L2TP menu
      ipsec      - IPsec menu
      comment    - Set comment
      del        - Remove group
```

Use the Group menu to define the user groups that reside on the VPN Gateway.

When a user logs in to the VPN (through 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 in the CLI, 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). To find a match, the system starts with applying group 1 (as defined in the CLI/BBI), then continues with group 2 and so on until all matches are found. The user is finally authenticated and mapped to one or several groups.

When the user requests a resource, the system tries to find a match between the requested resource and the access rules specified for the group(s). This done by checking each group in sequence according to the CLI/BBI order. Thus, the system starts by checking group 1's access rules in sequential order, that is, first Access rule 1, then Access rule 2 and so on. 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.

Note:

To shape a user's access rights depending on the user's connection specifics (for example source network or authentication method), extended profiles can be used. See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of groups, access rules and profiles.

Table 100: Group Menu Options (/cfg/vpn/aaa/group)

Command Syntax and Usage
name Assigns a name to the current user access group. When you have defined a name for the group, you can access the Group menu by specifying the group name instead of the group ID. The name you assign to the user group depends on which type of authentication mechanism you deploy. • RADIUS: The group name must correspond to an existing group name defined in the vendor-specific attribute used by the RADIUS server. Contact your RADIUS system administrator for information. • LDAP: The group name must correspond to an existing group name defined in the LDAP group attribute used by the LDAP server. Contact your LDAP system administrator for information. • NTLM: The group name must correspond to an existing group name in the Windows domain to which the user belongs. The most common examples of Windows domains to which a user belongs are "Domain Users", "Administrators", "Power Users" or "Guests". Note that these domains are different than User or Resource domains (that is, commonly domains that users log in to). Contact your Windows system administrator for more information. • SiteMinder: The group name must correspond to an existing group name defined in the SiteMinder group attribute used by the SiteMinder server. Contact your SiteMinder system administrator for information. • RSA SecurID. The group name must correspond to a group name defined for the RSA SecurID authentication method using the **/cfg/vpn <id>/aaa/ auth <id>/rsa/rsagroup** command. • RSA ClearTrust. The group name must correspond to a group name defined for the RSA ClearTrust authentication method on any of the ClearTrust authorization servers. • Client certificate: The group name must correspond to a group name defined as a group OID value in the client certificate (see the **/cfg/vpn <id>/aaa/ auth <id>/cert/groupoids** command) or to a group name mapped to a CA certificate (see the **/cfg/vpn <id>/aaa/ auth <id>/cert/ cacerts** command). • Local database: Any name can be used. The group name is only used internally for controlling access to intranet resources through the associated access rules. When adding a user to the local database, you map the user to one or more of the defined user access groups. **Note:** After you have assigned a name to the user access group, you must also define the access rules associated with the group. This must be done regardless of the authentication mechanism(s) that is used in the VPN.

Command Syntax and Usage
access
Displays the Access Rule menu.
spoaccess on|off
Sets Secure Portable Office feature access. • **on** Enable the SPO feature access in the server. • **off** Disable the SPO feature access in the server.
print

Displays an easy-to-read table overview of the access rights pertaining to the group. The table includes the Network, Ports, Proto (Protocol), Path and Action headings.
The example below shows a group whose access rights allow access to all networks, TCP ports, protocols and paths:
`Network  Ports      Proto Path  Action`
`-------  -----      ----- ----  ------`
`0.0.0.0/0 0           any   accept`

bwpolicy
Displays the referred BWM policy and allows you to change it. You can refer one of the BWM policies configured under **/cfg/bwm/bwmpolicy**. By default, it does not refer to any BWM policy.
restrict
Lets you specify the maximum number of simultaneous Portal/VPN sessions allowed for members of the current group. Example: If the value is set to 2, two simultaneous VPN sessions (that is, from two different computers) are allowed for a specific user. The default value is 0 = unlimited number of sessions.
usertype
Sets the user type for the current group. The user type determines which tabs will be available on the VPN Portal. Available user types are: • **advanced:** Displays all tabs on the Portal. • **medium:** Displays all tabs but the Advanced tab. • **:** Limits display to the Home tab (containing group links) and the Tools tab. If the user belongs to several groups with different user types assigned to them, the best user type will be selected upon user login. **Note:** The user type distinction has no impact on access rules or vice versa.

Command Syntax and Usage
idlettl <*value in seconds (s), minutes (m), hours (h) or days (d)*>
Sets the period during which a user's VPN session can be idle before the connection is automatically closed. This option helps prevent allocation of resources on the VPN Gateway for sessions that are no longer active. When 10% of the portal idle timeout is reached, a logout warning window is displayed. The window warns the user about the upcoming logout and offers to refresh the portal connection. If the portal connection is not refreshed, the user is automatically logged out. If the user is logged out, any sub windows or applets (for example port forwarders) opened during the Portal session are automatically closed. The idle timeout value can be set on VPN level as well, using the **/cfg/vpn <id>/aaa/idlettl** command. When the user logs in, the best idle timeout value configured for the user's different groups and the VPN's timeout value is selected. Example: If the user belongs to only one group and no idle timeout value is configured on group level (using this command), the value is 0. This means that the idle timeout value configured on VPN level will be used, because this value can never be lower than 2m (2 minutes). The default value and minimum value is 0. The maximum value is 31 days (31d).
sessionttl <*value in minutes (m), hours (h) or days (d)*>
Sets the maximum length of a group member's VPN session. The user will be logged out after this time has expired, regardless if he is active or not. The session timeout value can be set on VPN level as well, using the **/cfg/vpn <id>/aaa /sessionttl** command. When the user logs in, the best session timeout value configured for the user's different groups and the VPN's default timeout value is selected. Example: If the user belongs to only one group and no session timeout value is configured on group level (using this command), the value is 0. This means that the session timeout value configured on VPN level will be used, because this value can never be lower than 2m (2 minutes). The default value and minimum value is 0. The maximum value is (31d) 31 days or infinity.
vpnadmin true|false
Enables/disables the right to configure the VPN from the Browser-Based Management Interface (BBI) for members of the current group. • **true.** The VPN Administration option (link to BBI) is added to the Portal's Tools tab for all members of this group. • **false.** Administration through the BBI is not possible. To enable VPN administration through the BBI globally for the VPN, also set the **/cfg/vpn <id>/adv/vpnadmin** command to **true**. **Note:** The **vpnadmin**command is only accessible if a Secure Service Partitioning license is loaded. For more information about the Secure Service Partitioning

Command Syntax and Usage
feature, see the "Secure Service Partitioning" chapter in the *Application Guide for VPN* . The default value is **false**.
ndwauser <*Windows administrator user name*>
Lets you configure the Windows administrator user name for members of the current group. To be able to install the Windows version of the Net Direct client (downloadable from the Portal), users have to be administrator users on their PCs. By storing the user name (and password) on the AVG, group members that do not have administrator privileges will be able to install Net Direct. If the user belongs to several groups, the first found combination of Windows administrator user name and password in the user's different groups will be used. The system checks the groups in sequential order as configured in the CLI/BBI. **Note:** By supplying the Windows administrator user name and password, the security in your Windows environment may be impaired. Carefully consider the risks before proceeding with this option. For more information about Net Direct, see /cfg/vpn <id>/sslclient Net Direct and SSL VPN Client Configuration on page 377.
ndwapasswo <*Windows administrator password*>
Lets you configure the Windows administrator password for members of the current group. To be able to install the Windows Net Direct client (downloadable from the Portal), users has to be administrator users on their PCs. By storing the password (and user name) on the AVG, group members that do not have administrator privileges will be able to install Net Direct. If the user belongs to several groups, the first found combination of Windows administrator user name and password in the user's different groups will be used. The system checks the groups in sequential order as configured in the CLI/BBI. For more information about Net Direct, see /cfg/vpn <id>/sslclient Net Direct and SSL VPN Client Configuration on page 377.
linkset
Displays the Linkset menu for mapping linksets to the current group. To view menu options, see /cfg/vpn <id> /aaa/group <id> /linkset Linkset Mapping Configuration on page 235.
sposwindex
Displays SPO Application index menu. To view menu options, see /cfg/vpn <id>/aaa/group <id>/sposwindex SPO software index menu on page 236.
extend
Display the Extended profile menu, after you have typed the index number or name of an existing profile or the index number of a new profile. To view existing profiles, press TAB following the **extend** command. To view menu options, see /cfg/vpn <id> /aaa/group <id > /extend <id> Extended Profile configuration on page 237.

Command Syntax and Usage
tgsrs <*SRS rule name*>
Maps a previously configured Tunnel Guard SRS rule to the current group. **Note:** SRS rules must be configured through the Browser-Based Management Interface (BBI). It is not possible to configure an SRS rule through the CLI. If a user belongs to several groups, the first found SRS rule in any of the user's groups is used. The system checks the groups for SRS rules in the order the order they are configured in the CLI. For more information about Tunnel Guard with configuration examples, see the "Configure Tunnel Guard" chapter in the *Application Guide for VPN* .
vdesktop
Allows virtual desktop setting for a group. Vdesktop settings are configured only for the base profile.
wiper on|off
This command is only visible if IE cache wiper support has been delegated to group level, that is, the **/cfg/vpn <id>/portal/wiper** command has been set to group . • **on:** Users belonging to the current group will have the option to download the IE cache wiper when logging in to the Portal (if using Internet Explorer). If downloaded, the IE cache wiper will clear the cache and browser history when the Portal session is terminated or when the browser is closed. Note that this only applies to HTML pages accessed through the Portal during the secure session. Previously cached content and history entries will not be cleared. • **off:** The IE cache wiper cannot be downloaded by the user. If the remote user belongs to several groups, the IE cache wiper is enabled if it is enabled for any of the groups. The default setting is **on**.
citrix on|off
This command is only visible if Citrix Metaframe support has been delegated to group level, that is, the **/cfg/vpn <id>/portal/citrix** command has been set to group. • **on:** When users belonging to the current group logs in to the Portal, a Java applet is started. The applet enables support for Citrix Metaframe web links on the Portal. The Portal link is easily created by simply specifying the URL to the Citrix Metaframe server with the **internal** link type (also see /cfg/vpn <id> / linkset <id> /link <id> /internal Internal Link Configuration on page 371). • **off:** Links to Citrix Metaframe servers are only supported if created by means of the **custom** port forwarder link type. If Citrix Metaframe links are not used, **off** is the recommended setting, because this saves the AVG from starting the Java applet that supports this feature.

Command Syntax and Usage
If the remote user belongs to several groups, Citrix Metaframe support is enabled if it is enabled for any of the groups. **Note:** When **citrix** is set to on, the AVG supports rewrite of ICA files only. Other methods are possible but may require configuration changes on the Citrix Metaframe server side. The default setting is **off**.
netdirect on|off
This command is only visible if Net Direct support has been delegated to group level, that is, the **/cfg/vpn <id>/sslclient/netdirect** command has been set to **group**. • **on:** When members of the current group logs in to the Portal, Net Direct will be enabled. To activate Net Direct, the remote user can for example click the Net Direct link on the Portal. This gives the user the possibility to start a native client application (for example Outlook Express) and connect to a remote host through a secure SSL connection. • **off:** Net Direct will not be enabled for members of the current user group. If the user belongs to several groups, Net Direct will be enabled if it is enabled for any of the user's different groups. The default setting is **off**.
ippool *<ip pool number>*
Lets you reference a previously created IP pool number. The settings made for this IP pool will apply when a member of the current group logs in to the VPN. The IP pool comes into play when a remote user tries to establish a connection using the Avaya VPN client (formerly the Contivity VPN client) or the Net Direct client. A new source IP address has to be assigned to the unencrypted connection between the AVG and the requested resource and the IP pool settings determine whether the IP address is assigned from a local pool of IP addresses, from an external RADIUS server or from an external DHCP server. The IP pool is configured with the **/cfg/vpn <id>/ippool** command (see /cfg/vpn <id> /ippool <id> IP Pool Configuration on page 307). If no IP pool is assigned to the group, the default IP pool will be used (configured under **/cfg/vpn <id>/aaa/defippool**). If the user belongs to several groups, the first found IP pool (if any) in the user's different groups will be used. The groups are checked in the order they are configured in the CLI/BBI.
hippool <host ip pool number>
Lets you reference a previously created host IP pool number. The settings made for this host IP pool applies when a member of the current group logs on to the VPN. The host IP pool comes into play when a remote user tries to establish a connection using the Avaya VPN client (formerly the Contivity VPN client) or the Net Direct

Command Syntax and Usage
client. A new source host IP address is assigned to the unencrypted connection between the AVG and the requested resource and the host IP pool settings determine whether the host IP address is assigned from a local pool of host IP addresses, from an external RADIUS server or from an external DHCP server. The IP pool is configured with the **/cfg/vpn <id>/hippool** command. For more information about the configuration, see /cfg/vpn <id>/hippool Host IP Pool Configuration on page 313. If the user belongs to several groups, the first found host IP pool (if any) in the user's different groups is used. The groups are checked in the order they are configured in the CLI or BBI.
l2tp
Displays L2TP menu for setting the shared secret and the desired user tunnel profile for the current group. To view the menu options, see /cfg/vpn <id>/aaa/group/l2tp L2TP Group Configuration on page 241.
ipsec
Displays the IPsec menu for setting the shared secret and the desired user tunnel profile for the current group. To view menu options, see /cfg/vpn <id> /aaa/group <id> /ipsec IPsec Group Configuration on page 242. **Note:** This command is not available if the VPN Gateway software is run on the ASA 310 or ASA 410 hardware platforms.
comment
Lets you enter a comment for the current group.
del
Removes the user access group from the current VPN. **Note:** All access rules associated with the current group ID will be deleted as well.
splitnets
Configures split networks in the matching group for the user. This command will be visible only if /cfg/vpn <id>/sslclient/netdirect has been set to group, and /cfg/vpn <id>/aaa/group <id>/netdirect has been set to on.

/cfg/vpn <id> /aaa/group <id> /access <rule number> Access Rule Configuration

```
[Access rule 1 Menu]
network    - Set network reference
service    - Set service reference
appspec    - Set application specific reference
action     - Set action
comment    - Set access rule comment
del  - Remove access rule
```

The Access rule menu is used to 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.

Since the access rules are applied in sequential order, the order in which the access rules are configured could be important. For example, if a network definition is used to deny access to a specific host on a network, this access rule should be configured with a lower sequence number than an access rule allowing access to that network.

See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of groups, access rules and profiles.

Table 101: Access Rule Menu Options (/cfg/vpn/aaa/group/access)

Command Syntax and Usage
network Lets you reference a previously configured network definition (which may contain several host and subnet definitions). To view existing network definitions, press TAB following the **network** command. Example: To restrict access to a specific subnet, reference the network name whose definition corresponds to that subnet. To configure a network definition, use the **/cfg/vpn <id>/aaa/network** command.
service Lets you reference a previously configured service definition (which may contain several port and protocol definitions). To view available services, press TAB following the **service** command.

Command Syntax and Usage
Example: To restrict access to a specific application, reference the service name whose definition corresponds to that application's well-known port number. To configure a service, use the **/cfg/vpn <id>/aaa/service** command.
appspec
Lets you reference a previously configured appspec definition. An appspec definition identifies a path, e.g. **/public**. To view available appspec entries, press TAB following the **appspec** command. Example: To restrict access to a specific subdirectory on a host, reference the appspec entry that identifies the desired path. To configure an appspec definition, use the **/cfg/vpn <id>/aaa/appspec** command.
action accept|reject
Sets the action that is triggered when an SSL VPN user's request results in a match. • **accept:** The user's request is accepted, and access to the resource is granted. • **reject:** The user's request is rejected, and the browser displays an error message. The default action setting is **reject.**
del
Removes the current access rule from the group.

/cfg/vpn <id> /aaa/group <id> /linkset Linkset Mapping Configuration

```
 [Linksets Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The Linksets menu is used to map linksets to the current group. A linkset consists of one or several Portal links, defined with the **/cfg/vpn <id>/linkset #/link** command. The same linkset can be mapped to several groups. If a remote user belongs to several groups, all links in all linksets pertaining to the user's different groups will displayed on the Portal's Home tab when the user logs in.

Table 102: Linksets Menu Options (/cfg/vpn/aaa/group/linkset)

Command Syntax and Usage
list
Lists the currently configured linksets by index number.
del
Removes the linkset entry that is represented by the index number you specify. Use the **list** command to view all entries and related index numbers currently added to the list.
add
Lets you add a new linkset to the current group.
insert
Lets you assign a specific index number to the linkset entry you add. The index number you specify must be in use. Linkset entries with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move
Lets you move a linkset entry up or down in the list. To view all linkset entries, use the **list** command.

/cfg/vpn <id>/aaa/group <id>/sposwindex SPO software index menu

```
[SPO SW Index Menu]

list            - List all values

del             - Delete a value by number

add             - Add a new value
```

The following table shows the command syntax for the command **/cfg/vpn <id>/aaa/group <id>/sposwindex.**

Table 103: SPO software index menu (/cfg/vpn <id>/aaa/group <id>/sposwindex)

Command Syntax and Usage
list
Display all the SPO Application index menu.
del
Remove SPO Application index from the menu.
add
Add a SPO software index to the list.

/cfg/vpn <id> /aaa/group <id > /extend <id> Extended Profile configuration

```
[Extended Profile 1 Menu]
filter     - Set client filter reference
access     - Access rule menu
print- Print access rules
usertype   - Set portal user type
idlettl    - Set login session idle time
sessionttl - Set maximum session length
vpnadmin   - Allow VPN administration to group
ippool     - Set IP pool
hostippool - Set Host IP pool
linkset    - Linkset menu
wiper- Set use ActiveX component for clearing cache
citrix     - Set Citrix support
netdirect  - Allow Netdirect client
del  - Remove profile
```

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

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

The extended profile's data is applied when the user's connection specifics (for example authentication method or source network) matches the client filter referenced in the extended profile. For example, if the remote user authenticates to the VPN Gateway through a secure method, the access rules defined in the extended profile could be more generous.

The client filter identifies one or several of the following security aspects related to the user's connection:

- source network (for example a branch office network)
- authentication method (for example RADIUS)
- access method (SSL, IPsec, Net Direct, and/or SPO)
- client certificate installed (yes/no)
- IE cache wiper installed (yes/no)
- Tunnel Guard checks passed (yes/no)

For more information about the different client filter types, see /cfg/vpn <id> /aaa/filter <id> Client Filter Configuration on page 222.

For examples on how to apply client filters and extended profiles, see the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN*.

Table 104: Extended Profile Menu Options (/cfg/vpn/aaa/group/extend)

Command Syntax and Usage
filter *<reference to previously defined client filter>* Lets you reference a previously defined client filter to be used in the current extended profile. Whenever a match is found between a user's source network or authentication method and the source network or authentication method used by the client filter, the extended profile's data is applied. To view available client filters, press TAB following the **filter** command. Example: You have previously defined a client filter identifying a client network, called branchoffice. By referencing this client filter, the extended profile will be applied when the group member accesses the VPN Gateway from that branch office. To configure a client filter, use the **/cfg/vpn <id>/aaa/filter** command.
access Displays the Access rule menu, after you have typed the index number of an existing access rule or a new access rule. To view existing access rules, press TAB following the **access** command. To view menu options, see /cfg/vpn <id> /aaa/group <id> /access <rule number> Access Rule Configuration on page 234. The Access rule menu options for extended profiles are the same as for base profiles, that is, data specified directly under the Group menu.
print Displays an easy-to-read table overview of the access rules pertaining to the extended profile. The table includes the Network, Ports, Proto (Protocol), Path and Action headings.
usertype

Command Syntax and Usage
Sets the user type for the current extended profile. The user type determines which tabs will be available on the VPN Portal. Available user types are: • **advanced:** Displays all tabs on the Portal. • **medium:** Displays all tabs but the Advanced tab. • **:** Limits display to the Home tab (containing group links) and the Tools tab.
idlettl *<value in seconds (s), minutes (m), hours (h) or days (d)>*
Sets the period during which a user's VPN session can be idle before the connection is automatically closed. This option helps prevent allocation of resources on the VPN Gateway for sessions that are no longer active. The idle timeout value can be set on VPN level as well, using the **/cfg/vpn <id>/aaa /idlettl** command. It can also be set on group level, using the **/cfg/vpn <id>/aaa /group <id>/idlettl** command. When the user logs in, the best idle timeout value configured for the user's different groups, matching extended profile and the VPN's default timeout value will be selected.
sessionttl *<value in minutes (m), hours (h) or days (d)>*
Sets the maximum length of a remote user's VPN session. The user will be logged out after this time has expired, regardless if he is active or not. The session timeout value can be set on VPN level as well, using the **/cfg/vpn <id>/aaa /sessionttl** command. It can also be set on group level, using the **/cfg/vpn <id>/aaa /group <id>/sessionttl** command. When the user logs in, the best session timeout value configured for the user's different groups, matching extended profile and the VPN's default timeout value will be selected.
vpnadmin true|false
Enables/disables the right to configure the VPN from the Browser-Based Management Interface (BBI). • **true.** Enables administration rights through the BBI. The VPN Administration option (link to BBI) is added to the Tools tab on the Portal. • **false.** Disables administration rights through the BBI. **Note:** The **vpnadmin** command is only accessible if a Secure Service Partitioning license is loaded. For more information about the Secure Service Partitioning feature, see the "Secure Service Partitioning" chapter in the *Application Guide for VPN*. The default value is **false.**
ippool *<ip pool number>*

Command Syntax and Usage
Lets you reference a previously created IP pool number. The settings made for this IP pool will apply when a user assigned to the current extended profile logs in to the VPN. The IP pool comes into play when a remote user tries to establish a connection using the Avaya VPN client (formerly the Contivity VPN client) or the Net Direct client. A new source IP address has to be assigned to the unencrypted connection between the AVG and the requested resource and the IP pool settings determine whether the IP address is assigned from a local pool of IP addresses, from an external RADIUS server or from an external DHCP server. The IP pool is configured with the **/cfg/vpn <id>/ippool** command (see /cfg/vpn <id> /ippool <id> IP Pool Configuration on page 307).
hippool <*host ip pool number*>
Lets you reference a previously created host IP pool number. The settings made for this host IP pool applies when a user assigned to the current extended profile logs in to the VPN. The host IP pool comes into play when a remote user tries to establish a connection using the Avaya VPN client (formerly the Contivity VPN client) or the Net Direct client. A new source host IP address is assigned to the unencrypted connection between the AVG and the requested resource and the host IP pool settings determine whether the host IP address is assigned from a local pool of the host IP addresses, from an external RADIUS server or from an external DHCP server. The host IP pool is configured with the **/cfg/vpn <id>/hippool** command. For more information about the configuration, see /cfg/vpn <id>/hippool Host IP Pool Configuration on page 313.
linkset
Displays the Linkset menu for mapping linksets to the current extended profile. To view menu options, see /cfg/vpn <id> /aaa/group <id> /linkset Linkset Mapping Configuration on page 235.
wiper on|off
This command is only visible if IE cache wiper support has been delegated to group level, that is, the **/cfg/vpn <id>/portal/wiper** command has been set to **group**. • **on:** Users assigned to the current extended profile will have the option to download the IE cache wiper when logging in to the Portal (if using Internet Explorer). If downloaded, the IE cache wiper will clear the cache and the visited URLs list when the Portal session is terminated or when the browser is closed. Note that this only applies to HTML pages accessed through the Portal during the secure session. Previously cached content and history entries will not be cleared. • **off:** The IE cache wiper cannot be downloaded by the user. The default setting is **on**.
citrix on|off

Command Syntax and Usage
This command is only visible if Citrix Metaframe support has been delegated to group level, that is, the **/cfg/vpn <id>/portal/citrix** command has been set to **group**. • **on:** When users assigned to the current extended profile logs in to the Portal, a Java applet is started. The applet 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 link type (also see /cfg/vpn <id> /linkset <id> /link <id> /internal Internal Link Configuration on page 371). • **off:** Links to Citrix Metaframe servers are only supported if created by means of the custom port forwarder link type. If Citrix Metaframe links are not used, **off** is the recommended setting, because this saves the AVG from starting the Java applet that supports this feature. **Note:** When **citrix** is set to **on**, the AVG supports rewrite of ICA files only. Other methods are possible but may require configuration changes on the Citrix Metaframe server side. The default setting is **off.**
netdirect on|off
This command is only visible if Net Direct support has been delegated to group level, that is, the **/cfg/vpn <id>/sslclient/netdirect** command has been set to **group**. • **on:** When users assigned to the current extended profile logs in to the Portal, Net Direct will be enabled. To activate Net Direct, the remote user can for example click the Net Direct link on the Portal. This gives the user the possibility to start a native client application (for example Outlook Express) and connect to a remote host through a secure SSL connection. • **off:** Net Direct will not be enabled for members of the current user group. The default setting is **off.**
del
Removes the current extended profile from the group.

/cfg/vpn <id>/aaa/group/l2tp L2TP Group Configuration

```
[L2tp Menu]
      secret     - Set shared secret
      utunnel    - Set user tunnel profile
```

The Layer 2 Tunneling Protocol (L2TP) menu is used to enter a shared secret for L2TP clients authenticating to the L2TP server with group authentication. You can map a previously defined user tunnel profile to the current group. If the user belongs to several groups, the first found

combination of shared secret or user tunnel profile in the user's different groups is used. The groups are checked in the order they are configured in the CLI and BBI.

Table 105: L2TP Menu options (/cfg/vpn/aaa/group/l2tp

Command Syntax and Usage
secret <*shared secret*> Sets the shared secret for clients authenticating to the L2TP server with group authentication. The shared secret provided here must be equal to the shared secret or password configured for group authentication in the L2TP client.
utunnel Lets you map a previously configured user tunnel profile to the current group. The user tunnel profile defines the encryption and tunnel handling parameters to be used when members of the current group set up an L2TP tunnel to the VPN Gateway.

/cfg/vpn <id> /aaa/group <id> /ipsec IPsec Group Configuration

```
[IPsec Menu]
secret     - Set shared secret
utunnel    - Set user tunnel profile
```

The IPsec menu is used to enter a shared secret for IPsec clients authenticating to the IPsec server with group authentication. This is also where you map a previously defined user tunnel profile to the current group. If the user belongs to several groups, the first found combination of shared secret/user tunnel profile in the user's different groups will be used. The groups are checked in the order they are configured in the CLI and BBI.

Note:

This menu is not available if the VPN Gateway software is run on the ASA 310 or ASA 410 hardware platforms.

Table 106: IPsec Menu Options (/cfg/vpn/aaa/group/ipsec)

Command Syntax and Usage
secret <*shared secret*> Sets the shared secret for clients authenticating to the IPsec server (the VPN Gateway) with group authentication. The shared secret entered here must be equal to the shared secret/password configured for group authentication in the Avaya VPN client (formerly Contivity).

Command Syntax and Usage
Note: If user name and password authentication is used (ISAKMP tunnel), a shared secret is not required. This login type however requires that the user is configured in the AVG's local database, using the **/cfg/vpn <id>/aaa/auth <id>/local/add** command.
utunnel
Lets you map a previously configured user tunnel profile to the current group. The user tunnel profile defines the encryption and tunnel handling parameters to be used when members of the current group sets up an IPsec tunnel to the VPN Gateway. For instructions on how to configure a user tunnel profile, see /cfg/vpn <id>/ipsec IPsec Configuration on page 282.

/cfg/vpn <id> /aaa/ssodomains Single-Sign-On Domain Configuration

```
[SSO Domains Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
```

The SSO (Single Sign-On) Domains menu lets you configure domains for which single-sign-on is allowed. The VPN Gateway will automatically log in remote users to hosts in the specified domains, provided the required credentials are identical with those entered at Portal login. The feature supports web servers using HTTP-based authentication (basic or NTLM), as well as FTP and SMB (Windows file share) file servers.

Auto-login takes place whenever the remote users tries to access a password-protected web page or file server during the Portal session, for example through the URL field, a link on the Portal's Home tab or any other web link accessed during the session.

Note that the SSO domains feature supports automatic login to all servers in the specified domain. For a more restricted approach – where access to a server can be specified down to path level – use the iauto link instead. The iauto link also supports form-based authentication (see Link Configuration on /cfg/vpn <id> /linkset <id> /link <id> Link Configuration on page 333).

Table 107: SSO Domain Menu Options (/cfg/vpn/aaa/ssodomains)

Command Syntax and Usage
list

Command Syntax and Usage
Lists the currently configured SSO domains along with their corresponding index numbers.
del
Removes the specified SSO domain from the configuration by index number. Use the **list** command to display the index numbers of all added SSO domains.
add *<domain name or IP address> <basic mode>*
Adds an SSO domain name or IP address to the configuration. • Domain name or IP address. Enter the domain name, e.g. example.com. This will allow single sign-on to all servers matching the specified domain suffix, e.g. to www.example.com or test.lab.example.com. As an alternative, an IP address can be entered, e.g. 10.1.0.10, to limit single sign-on to a specific server. • Basic mode. Lets you select the desired mode for basic, HTTP-based authentication (popup window with user name and password fields). This setting is ignored for FTP and SMB file servers. - **normal:** For web servers requiring user name and password only. - **add_domain:** Some web servers require a domain name in addition to the user name to be inserted in the user name field. Example: User: <domain> \<user> Password: <password> The domain name added to the user name field will be the one specified for the relevant authentication method with the **/cfg/vpn <id>/aaa/auth <id>/domain** command. To add an additional SSO domain, use the **add** command once again. The next available index number is assigned automatically by the system.

/cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration

```
[SSO headers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The SSO headers menu is used to define custom single-sign on HTTP headers, for example for web servers that do not support basic or form-based authentication. The headers are added to all requests going to the specified backend server or domain. Note that the backend web server must be modified to support single-sign on through HTTP headers.

Table 108: SSO Headers Menu Options (/cfg/vpn/aaa/ssoheaders)

Command Syntax and Usage
list
Lists the currently configured SSO headers along with their corresponding index numbers.
del
Removes the specified SSO header from the configuration by index number. Use the **list** command to display the index numbers of all added SSO headers.
add <*host/domain*> <*header pattern*>
Lets you specify a single-sign on domain and a custom single-sign on header. • Host or domain, e.g. www.example.com or example.com. • Header pattern. Lets you define a custom header to be included in requests to the specified host or to hosts in the specified domain. Example 1: Enter **X-single-sign-on: user=<var:user> id=<var:password>**, to create a custom header that reads `X-single-sign-on: user=john id=secret` . The variables <var:user> and <var:password> expand to the credentials given by the remote user at Portal login. Example 2: To create a base 64 encoded MD5 checksum of the user name and password, include the <md5:string> variant, e.g. **X-single-sign-on: user=<var:user> credentials=<md5:<var:password>>** Example 3: To create a base 64 encoded string of the user name and password, include the <base64:string> variant, e.g. **X-single-sign-on: user=<var:user> credentials=<base64:<var:password>>** For the variables, all matching entries will be used so it is possible to add several headers to each request. Available variables are <*var:user*>, <*var:password*>, <*var:group*>, <*var:domain*>, <*var:sslsid*>, <*var:portal*>, <*var:method*> and all variables defined by the operator (for retrieving values from RADIUS or LDAP databases). See Variables on page 28.
insert <*index number to insert at*> <*host/domain to add*> <*pattern*>
Assigns a specific index number to the SSO header you add. The index number you specify must be in use. SSO headers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves an SSO header up or down in the list of configured headers. The index numbers you specify must be in use. To view all headers currently added to the configuration, use the **list** command.

/cfg/vpn <id> /aaa/radacct RADIUS Accounting Configuration

```
[Radius Accounting Menu]
servers    - RADIUS accounting servers menu
vpnattribu - VPN attribute menu
ena  - Enable RADIUS accounting
dis        - Disable RADIUS accounting
```

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. With a RADIUS accounting server configured, an accounting request start packet will be sent to the accounting server for each user that successfully authenticates to the AVG. The start packet contains the following information:

- Client user name
- The VPN Gateway's 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

The RADIUS server should be configured according to the recommendations in RFC 2866.

Note:

Using the **/cfg/vpn <id>/adv/log** command, the VPN Gateway can be configured to generate detailed log messages to a syslog server. The messages include information about Portal activities, for example visited URLs, rejects and so on.

Table 109: RADIUS Accounting Menu Options (/cfg/vpn/aaa/radacct)

Command Syntax and Usage
servers Displays the RADIUS accounting servers menu. To view menu options, see /cfg/vpn <id> /aaa/radacct/servers RADIUS Accounting Servers Configuration on page 247.
vpnattribu Displays the VPN Attribute menu. To view menu options, see /cfg/vpn <id> /aaa/radacct/vpnattribu VPN Attribute Configuration on page 248.

Command Syntax and Usage
ena
Enables RADIUS accounting.
dis
Disables RADIUS accounting.

/cfg/vpn <id> /aaa/radacct/servers RADIUS Accounting Servers Configuration

```
[Radius Accounting Servers Menu]
list       - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The RADIUS Accounting Servers menu is used to add one or more RADIUS accounting servers to the current configuration.

Table 110: RADIUS Accounting Servers Menu Options (/cfg/vpn/aaa/radacct /servers)

Command Syntax and Usage
list Lists the IP addresses of currently configured RADIUS accounting servers, along with their corresponding index numbers.
del Removes the specified RADIUS accounting server from the configuration. Use the **list** command to display the index numbers of all added RADIUS accounting servers.
add *<IP address> <TCP port number> <shared secret>* Adds a RADIUS accounting server to the configuration. Specify the IP address, a TCP port number, and the shared secret. The next available index number is assigned automatically by the system. **Note:** The default port number used for RADIUS accounting is 1813.
insert *<index number to insert at> <IP address of RADIUS accounting server to add>*

Command Syntax and Usage
Assigns a specific index number to the RADIUS accounting server you add. The index number you specify must be in use. RADIUS accounting servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves a RADIUS accounting server up or down in the list of configured servers. The index numbers you specify must be in use. To view all servers currently added to the configuration, use the **list** command.

/cfg/vpn <id> /aaa/radacct/vpnattribu VPN Attribute Configuration

```
[VPN Attribute Menu]
vendorid   - Set vendor id for the VPN attribute
vendortype - Set vendor type for the VPN attribute
```

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 RADIUS accounting server (together with the accounting information for the logged in user). This way, accounting information can be separated per VPN.

Table 111: VPN Attribute Menu Options (/cfg/vpn/aaa/radacct/vpnattribu)

Command Syntax and Usage
vendorid
Assigns the SMI Network Management Private Enterprise Code—as defined by IANA in the file http://www.iana.org/— to the Vendor-Id attribute. The Vendor-Id—represented by the private enterprise number—is a value for RADIUS' standard attribute **vendor-specific** (26). If you want to use a standard attribute type as defined in RFC 2865, set **vendorid** to 0. Then configure the desired standard attribute type as the vendor type value (see next command). **Note:** If another Vendor-Id is used by your RADIUS system, you can use the **vendorid** command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. The default vendor-Id is **1872** (Alteon).
vendortype
Assigns a number to the Vendor-Type attribute used in RADIUS.

Command Syntax and Usage
Used in combination with the Vendor-Id number, the Vendor-Type number identifies the attribute which will contain the accounting information. Tip! Finding accounting entries in the RADIUS server's log can be made easier by defining a suitable string in the RADIUS server's dictionary (for example Alteon-Portal-ID) and mapping this string to the vendor type value. **Note:** If another number for vendor type is used by your RADIUS system, you can use the **vendortype** command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. The default vendor type value is 3.

/cfg/vpn <id>/aaa/adv Advanced Group Menu

```
[Advanced Group Menu]
      unmatchgrp - Unmatched group menu
```

Table 112: Advanced Group Menu Options (/cfg/vpn/aaa/adv)

Command Syntax and Usage
unmatchgrp Displays Unmatched Group Menu. To view menu options, see /cfg/vpn <id>/aaa/adv/unmatchgrp Unmatched Group Menu on page 249.

/cfg/vpn <id>/aaa/adv/unmatchgrp Unmatched Group Menu

```
[Unmatched Group Menu]
      defgroup   - Set unmatched group mapping
      ena        - Enable unmatched group mapping
      dis        - Disable unmatched group mapping
```

Table 113: Advanced Group Menu Options (/cfg/vpn/aaa/adv)

Command Syntax and Usage
defgroup Lets you define unmatched group mapping. You can define a group that matches users based on the null value in the RADIUS and LDAP fields. This makes most of the users to come under the default group option. For LDAP users, a specified group LDAP Auth applies with the default group.
ena

Command Syntax and Usage
Enable unmatched group mapping.
dis
Disable unmatched group mapping.

/cfg/vpn <id> /server Portal Server Configuration

```
[Server Menu]
      port       - Set listen port of server
      dnsname    - Set DNS name of server
      trace      - Traffic trace menu
      ssl        - SSL settings menu
      tcp        - TCP endpoint settings menu
      http       - HTTP settings menu
      proxymap   - Intranet proxy configuration menu
      portal     - Portal settings menu
      adv        - Advanced settings menu
      ena        - Enable virtual server
      dis        - Disable virtual server
```

The Server menu is used to configure the portal server used in the current VPN. The default SSL, TCP and HTTP values need normally not be changed.

Table 114: Server Menu Options (/cfg/vpn/server)

Command Syntax and Usage
port <*TCP port number*> Sets the TCP port number to which the portal server should listen. The default is port 443.
dnsname <*fully qualified domain name of the Portal IP address*>
Assigns a DNS name to the Portal IP address, e.g. vpn.example.com. Generally, a DNS name is only required if your DNS server is unable to perform reverse lookups of the Portal IP address (for example in a testing environment) and if iauto links are used in conjunction with the HTTP Proxy applet. For more information about the iauto link and the HTTP Proxy applet, see /cfg/vpn <id> /linkset <id> /link <id> /iauto Iauto Link Configuration on page 372. When pressing Return after having specified the DNS name, a check will be performed against the DNS server included in the system configuration (see the **/cfg/sys/dns** command). The system tries to verify that the fully qualified domain name you have specified is registered in DNS, and that the resolved IP address corresponds to the virtual server IP address.
trace
Displays the Trace menu. To view menu options, see /cfg/vpn <id> /server/trace Trace Configuration on page 251.
ssl

Command Syntax and Usage
Displays the SSL settings menu. To view menu options, see /cfg/vpn <id> /server/ssl SSL Settings Configuration on page 253.
tcp
Displays the TCP settings menu. To view menu options, see /cfg/vpn <id> /server/tcp TCP Settings Configuration on page 256.
http
Displays the HTTP settings menu. To view menu options, see /cfg/vpn <id> /server/http HTTP Settings Configuration on page 258.
proxymap
Displays the Proxy Mapping menu. To view menu options, see /cfg/vpn <id> /server/proxymap Proxy Mapping Configuration on page 264.
portal
Displays the Portal settings menu. To view menu options, see /cfg/vpn <id> /server/portal Portal Server Settings Configuration on page 266.
adv
Displays the Advanced settings menu. To view menu options, see /cfg/vpn <id> /server/adv Advanced Settings Configuration on page 268.
ena
Enables the SSL functionality on the portal server.
dis
Disables the SSL functionality on the portal server. **Note:** Only the VPN's SSL functionality is disabled. If you have previously enabled IPsec (using the **/cfg/vpn <id>/ipsec/ena** command, this setting is not affected.

/cfg/vpn <id> /server/trace Trace Configuration

```
[Trace Menu]
      ssldump    - Create traffic dump
      tcpdump    - Create traffic dump
      ping       - Ping through backend interface
      dnslookup  - Lookup a name in DNS through backend interface
      traceroute - traceroute through backend interface
```

The Trace menu is used for capturing and analyzing SSL and TCP traffic flowing between clients and the portal server. The commands can be useful for debugging purposes. The

ssldump command will decrypt transmitted data traffic, provided private keys and certificates have been configured properly on the selected virtual SSL server.

The **ssldump** and the **tcpdump** commands can be permanently deactivated in the AVG cluster. For more information, see the **/cfg/sys/distrace** command on page distrace.

Table 115: Trace Menu Options (/cfg/vpn/server/trace)

Command Syntax and Usage
ssldump interactive|tftp|ftp|sftp Creates a dump of the SSL traffic flowing between clients and the portal server. The captured information can either be displayed decrypted on screen (the default interactive output mode), or saved as a file to a TFTP/FTP/SFTP server. The server can be specified using either the host name or the IP address. If you choose to send the dump as a file to a TFTP server, a number of files will be sent to the server depending on the amount of captured information. A number is appended to the file name given in the CLI, starting at 1 and incremented automatically for additional files. You will be prompted for a destination file name prefix of your own choice. If you choose to send the dump as a file to an FTP server, you will be prompted for the destination file name, as well as a user name and password valid on the specified FTP server. For detailed information about the default flags used when issuing the **ssldump** command, as well as customizing the default filter expression, see the SSLDUMP (1) manual pages under UNIX.
tcpdump interactive|tftp|ftp|sftp Creates a dump of the TCP traffic flowing between clients and the currently selected virtual SSL server. The captured information can either be displayed on screen (the default `interactive` output mode), or saved as a file to a TFTP/FTP/SFTP server. The server can be specified using either the host name or the IP address. You can read a saved TCP traffic dump file using the TCPDUMP or Ethereal application on a remote machine. If you choose to send the dump to a TFTP server, a number of files will be saved on the server depending on the amount of captured information. A number is appended to the file name given in the CLI, starting at 1 and incremented automatically for additional files. You will be prompted for a destination file name prefix of your own choice. If you choose to send the dump as a file to an FTP server, you will be prompted for the destination file name, as well as a user name and password valid on the specified FTP server. For detailed information about the default flags used when issuing the **tcpdump** command, as well as customizing the default filter expression, see the TCPDUMP (8) manual pages under UNIX.
ping <*host name or IP address*> Use this command to verify station-to-station connectivity across the network. If a backend interface is mapped to the current VPN, the check is made through that backend interface.

Command Syntax and Usage
To map a backend interface to the VPN, use the **/cfg/vpn <id>/adv/interface** command. To be able to use a host name, the DNS parameters must be configured. To configure a DNS server specific for the VPN, use the **/cfg/vpn <id>/adv/dns/servers** command or use the default DNS server **(/cfg/sys/dns)**.
dnslookup <*host name or IP address*>
Use this command to find the IP address or host name of a machine. If a backend interface is mapped to the current VPN, the check is made through that backend interface. If a DNS server is configured for the current VPN, the check is made against that DNS server. To map a backend interface to the VPN, use the **/cfg/vpn <id>/adv/interface** command. To configure a DNS server specific for the VPN, use the **/cfg/vpn <id> /adv/dns/servers** command.
traceroute <*host name or IP address of target station* >
Use this command to identify the route used for station-to-station connectivity across the network. If a backend interface is mapped to the current VPN, the check is made through that backend interface. To map a backend interface to the VPN, use the **/cfg/vpn <id>/adv/interface** command. To be able to use a host name, the DNS parameters must be configured. To configure a DNS server specific for the VPN, use the **/cfg/vpn <id>/adv/dns/servers**command or use the default DNS server **(/cfg/sys/dns)**.

/cfg/vpn <id> /server/ssl SSL Settings Configuration

```
[SSL Settings Menu]
      cert       - Set server certificate
      cachesize  - Set SSL cache size
      cachettl   - Set SSL cache timeout
      cacerts    - Set list of accepted signers of client certificates
      cachain    - Set list of CA chain certificates
      protocol   - Set protocol version
      log        - Set syslog detail for ssl connection
      verifylog  - Set syslog detail for client certificate
      ciphers    - Set cipher list
      verify     - Set certificate verification level
      ena        - Enable SSL
      dis        - Disable SSL
```

The SSL Settings menu is used for configuring SSL-specific settings for the portal server.

Table 116: SSL Settings Menu Options (/cfg/vpn/server/ssl)

Command Syntax and Usage
cert <*certificate index number*>

Command Syntax and Usage
Specifies which server certificate is used by the portal server. To view basic information about available certificates, use the **/info/certs** command. To add a new certificate, see the "Adding Certificates to the AVG " section in the "Certificates and Client Authentication" chapter in the *User's Guide*. Note that the server may only use one server certificate.
cachesize <*number of SSL sessions*>
Sets the size of the SSL cache. The default value is 4000 cached sessions. If you notice that there are many cache misses, the `cachesize` value can be increased for better performance. To view the number of cache misses for the portal server, use the **/stats/sslstats/vpn <id>/cachemisse** command.
cachettl <*maximum Time To Live value in seconds*>
Sets the maximum Time To Live (TTL) value for items in the SSL cache, before they are discarded. The default TTL value is 5 minutes.
cacerts <*certificate index number*>
Specifies which of the available CA certificates to use for client authentication. CA certificates are added the same way as an SSL server certificate – either through cut-and-paste or through TFTP/FTP/SCP/SFTP from a remote host. Both actions are performed from the Certificate menu. To get an overview over available certificates, enter the **/info/certs** command. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified CA certificates, press ENTER when asked to enter the certificate numbers, then answer yes to the question if you want to clear the list. **Note:** If you are using one of the available certificates to generate your own client certificates, you must specify it as a CA certificate to successfully authenticate clients. For more information on client authentication, see the section "Configuring a Virtual SSL Server for Client Authentication" in the "Certificates and Client Authentication" chapter in the *User's Guide*.
cachain <*certificate index number*>
Specifies the CA certificate chain of the server certificate. The chain starts with the issuing CA certificate of the server certificate, and can range up to the root CA certificate. This command explicitly constructs the server certificate chain, which is sent to the browser in addition to the server certificate. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified chain certificates, press ENTER when asked to enter the certificate numbers, then answer yes to the question if you want to clear the list.

Command Syntax and Usage
Note: When configuring the virtual SSL server to use chain certificates, the protocol version must be set to SSL3 or SSL23.
protocol ssl2|ssl3|ssl23|tls1|tls11|tls12
Specifies the protocol to use when establishing an SSL session with a client. Valid options are as follows: • **ssl2:** Only accept SSL 2.0. • **ssl3:** Only accept SSL 3.0. • **ssl23:** Accept SSL 2.0, SSL 3.0, and TLS 1.0. • **tls1**: Only accept TLS 1.0. • **tls11:** Only accept TLS 1.1. • **tls12:** Only accept TLS 1.2. The default protocol value is **ssl23.**
log none|accept|reject|both
Lets you specify SSL connection details for sending to syslog. • **none** • **accept** • **reject** • **none** The default verify value is **none**.
verify log none|accept|reject|both
Lets you specify the syslog detail for client certificate. • **none** • **accept** • **reject** • **none** The default verify value is **none**.
verify none|optional
Specifies the level of client authentication to use when establishing an SSL session. Valid options are as follows: • None: No client certificate is required. • Optional: A client certificate is requested, but the client need not present one.

Command Syntax and Usage
The default verify value is **none**.
ciphers <*cipher list*>
Lets you change the default cipher preference list, which corresponds to `ALL:-EXPORT:-LOW!ADH:-SSLv2 .` For more information about cipher lists, see the "Cipher List Formats" section in Appendix A, Supported Ciphers, in the *User's Guide*.
ena
Enables SSL on the portal server. SSL is enabled by default.
dis
Disables SSL on the portal server.

/cfg/vpn <id> /server/tcp TCP Settings Configuration

```
[TCP Settings Menu]
      cwrite     - Set client TCP write timeout
      ckeep      - Set client TCP keep alive timeout
      skeep      - Set socks client TCP keep alive heartbeat timeout
      sinterval  - Set socks client TCP keep alive heartbeat interval
      swrite     - Set server TCP write timeout
      sconnect   - Set server TCP connect timeout
      csendbuf   - Set client TCP send buffer size
      crecbuf    - Set client TCP receive buffer size
      ssendbuf   - Set server TCP send buffer size
      srecbuf    - Set server TCP receive buffer size
```

The TCP Settings menu is used for configuring various TCP timeout and buffer size settings on both the client and the portal server side.

Table 117: TCP Settings Menu Options (/cfg/vpn/server/tcp)

Command Syntax and Usage
cwrite <*client write timeout*> Sets the timeout value for how long the portal server should wait for a write operation towards the client(s) to complete. The default client write timeout value is 15m = 15 minutes.
ckeep <*client keep alive timeout*> Sets the timeout value for how long the portal server should wait before closing an idle session. The default client keep alive timeout value is 15m = 15 minutes.
skeep <*SSL VPN client keep alive timeout*>

Command Syntax and Usage
If the SSL VPN client stops communicating with the VPN Gateway, this timeout value determines for how long the SSL VPN client should be kept alive before the remote user is logged out. The default SSL VPN client keep alive timeout value is 2m = 2 minutes. The **skeep** command is only available for virtual servers of the socks type.
sinterval <*1-600 sec*>
Lets you to specify the time interval for socks client to send heartbeats. The time interval ranges from 1 to 600 seconds.
swrite <*server write timeout*>
Sets the timeout value for how long the portal server should wait for a write operation towards the backend server(s) to complete. The default server write timeout value is 15m = 15 minutes.
sconnect <*server connect timeout*>
Sets the timeout value for how long the portal server should wait for a server connection when trying to open a TCP connection. The default server connect timeout value is 30s = 30 seconds.
csendbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the client TCP send buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default client TCP send buffer setting is **auto.**
crecbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the client TCP receive buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default client TCP receive buffer setting is **auto.**
ssendbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the server TCP send buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default server TCP send buffer setting is **auto.**
srecbuf auto| <*buffer size (2000-100000 bytes)*>
Sets the size of the server TCP receive buffer. If you specify a size manually, the buffer size should not be set lower than the normal MTU size which is 1500 bytes. The default server TCP receive buffer setting is **6000.**

/cfg/vpn <id> /server/http HTTP Settings Configuration

```
[HTTP Settings Menu]
      downstatus - Set server down reply status
      rewrite    - SSL triggered rewrite menu
      securecook - Set add secure option to session cookie
      certcard   - Set enable extra secure smart card setting
      sslheader  - Add SSL header
      sslxheader - Add SSL header with serial in hex
      sslsidhead - Add SSL SID header
      addxfor    - Add X-Forwarded-For header
      addvia     - Add Via header
      addxisd    - Add HTTP-X-ISD debug header
      addclicert - Add Client-Cert as a HTTP header
      addnostore - Add no-cache/no-store HTTP header
      nocachehdr - Remove Cache Control HTTP header
      compress   - Set compress http data to the client
      allowimage - Allow image caching
      allowdoc   - Allow document caching
      allowscrip - Set allow script caching
      allowica   - Allow ICA file caching
      cmsie      - Set MSIE session termination bug workaround
      maxrcount  - Set max number of persistant client requests
      maxline    - Set max line length
      urlobscure - Set URL obfuscation
      sessionhdr - Add X-Nortel-SSL-SessionInfo Header
```

The HTTP Settings menu is used for configuring HTTP-specific settings for the portal server.

Table 118: HTTP Settings Menu Options (/cfg/vpn/server/http)

Command Syntax and Usage
downstatus unavailable|redirect|reset Sets the type of behaviour when the HTTP server is down. • **unavailable:** Sends a HTTP 503 "Service Unavailable" message to the client. • **redirect:** Lets you specify a redirect URL using the **downurl** command (see below). • **reset:** Lets the client try to access the server again. The default value is **unavailable.**
securecook on|off • **on:** The VPN Gateway sets the Secure attribute on the AVG session cookie and all Set-Cookie headers generated by backend servers. It directs the user agent to use only secure means to contact the origin server whenever it sends back this cookie. For more information, see RFC 2109. • **off:** The Secure attribute is not set. This may cause the AVG session cookie to leak to a trap site through HTTP. The default value is **on.**

Command Syntax and Usage
sslheader on|off
Specifies how the virtual SSL server handles the optional X-SSL header. When added, the X-SSL header contains information about the particular cipher suite that was used during the SSL session – information that can be logged on the web servers. The information can also be used for web application logical decisions concerning which cipher suites should be accepted. Such a decision would then override the default cipher suite setting for a virtual SSL server on the VPN Gateway. Example of an added X-SSL header: X-SSL: decrypted=true, ciphers="TLSv1/SSLv3 RC4-MD5" If you have configured the virtual SSL server to require client certificates, information about the certificate issuer, the certificate subject, and the serial number is extracted from the client certificate and added to the encryption information in the X-SSL header. The length of the Subject (and Issuer) DN is limited to 1000 characters. If it is longer it is truncated. Valid options for the **sslheader** command are: • **on:** An X-SSL header is added to the client request. • **off:** No X-SSL header is added to the client request. The default value is **on.**
sslxheader on|off
This command is almost identical to the **sslheader** command (see above), with the difference that the serial number will be in hexadecimal format (with up to 254 hexadecimal digits) instead of decimal format. Usage: If very long serial numbers are used, and/or hexadecimal representation is desired, change the **sslheader** command to off and the **sslxheader** command to on. The default value is **off.**
sslsidhead on|off
If set to **on**, the SSL session ID header is added to the client request. The default value is **off.**
addxfor on|off|anonymous|remove
Specifies how the virtual SSL server handles the optional X-Forwarded-For HTTP header. When added, the X-Forwarded-For header contains information about the peer IP address of the current client connection. This information can be used for enhanced logging purposes. Valid options for the **addxfor** command are: • **on:** An X-Forwarded-For header is added to the current client request. • **off:** No action whatsoever is taken regarding the X-Forwarded-For header.

Command Syntax and Usage
• **anonymous:** The peer IP address of the current client connection is hidden. • **remove:** The X-Forwarded-For header is removed, if present, from the current client request. The default value for the **addxfor** setting is **off.** **Note:** If there are more than one AVG in a cluster and transparent proxy is set to **off**, then firewall load balancing (on the Application Switch) must also be set to **off** for the **addxfor** feature to work.
addvia on|off|anonymous|remove
Specifies how the virtual SSL server handles the through HTTP header. When added, the through HTTP header contains information about the IP address of the virtual server on the Application Switch. Valid options for the **addvia** command are: • **on:** A through header is added to the current client request. • **off:** No action whatsoever is taken regarding the through header. • **anonymous:** The IP address of the virtual server is hidden. • **remove:** The through header is removed, if present, from the current client request. The default value for the **addvia** setting is **on.**
addxisd on|off
Specifies how the virtual SSL server handles the optional HTTP-X-ISD header. This header can be used for debugging purposes when end to end encryption or load balancing of backend servers is performed by the VPN Gateway. When added, the extra HTTP-X-ISD header contains information about the IP addresses of both the VPN Gateway that initiated the request and the responding backend server, the internal index number of the responding the backend server, whether connection pooling is enabled, the load balancing type and metric, and finally, whether end to end encryption was performed. Example of an added HTTP-X-ISD header: `HTTP-X-ISD: 192.168.128.25 192.168.100.1 index=2; pool=on; lb=all-roundrobin; type=http-https` Valid options for the **addxisd** command are: • **on:** An HTTP-X-ISD header is added to the client request. • **off:** No HTTP-X-ISD header is added to the client request. The default value for the **addxisd** setting is **off.**
addclicert on|off
Specifies how the virtual SSL server handles the optional X-Client-Cert HTTP header. When added, the VPN Gateway will insert the entire client certificate (in

Command Syntax and Usage
PEM format) as a multiline HTTP header. The backend web servers can then perform additional user authentication, based on the information in the client certificate. The backend servers can also make use of any auxiliary fields in the client certificate. Valid options for the **addclicert** command are: • **on:** An extra X-Client-Cert HTTP header is added to the client request. • **off:** No extra X-Client-Cert HTTP header is added to the client request. The default value is **off.**
addnostore on|off
Specifies how the virtual SSL server handles the Cache-Control header in a HTTP 1.1 client connection request, or the Pragma header in a HTTP 1.0 client connection request. When added, the inadvertent release or retention of sensitive information is prevented by not allowing any part of the message to be stored in non-volatile storage. Information stored in volatile storage is removed as promptly as possible after having been forwarded. Valid options for the **addnostore** command are: • **on:** A Cache-Control: no-store general-header is added to a client HTTP 1.1 request, and a Pragma: no-cache general-header is added to a client HTTP 1.0 request. • **off:** No Cache-Control or Pragma header is added to the client request. The default value is **on** for all virtual SSL servers of the http and portal types.
nocachehdr on|off
Removes cache-control HTTP header. Valid options for the **nocacheldr** command are: • **on:** Cache-Control HTTP header is not added to the client request. • **off:** Cache-Control HTTP header is added to the client request. The command is available for virtual SSL servers of the http type. The default value is **off**.
compress on|off
Lets you enable compression of HTTP data (scripts and HTML) to the clients. • **on:** Scripts and HTML are compressed to enable faster HTTP data transfer to the clients. This may however reduce the encryption throughput on the AVG because the CPU will also be engaged in data compression. • **off:** No compression of HTTP data to clients is performed. The default setting is **off.**
allowimage on|off
Specifies whether or not to allow caching of images.

Command Syntax and Usage
• **on:** No-cache/no-store headers for images are not added. • **off:** No-cache/no-store headers for images are added. The default value is **on.**
allowdoc on|off
Specifies whether or not to allow caching of PDF, Word and Excel documents when clicking document links on intranet web pages during a portal session. To be able to open a document through Internet Explorer, this setting should be set to **on.** However, for security reasons you might want to turn caching of documents **off** (default value). You can still save a document to your computer by right-clicking it and selecting Save target as. • **on:** No-cache/no-store headers for documents are not added. • **off:** No-cache/no-store headers for documents are added. The default value is **off.** **Note:** When the **/cfg/vpn <id>/portal/wiper** command is set to **on** (default value), caching of documents is possible and the browser cache is cleared after the session (if Internet Explorer is used). In this case the default **allowdoc** setting can be kept.
allowscrip
Specifies whether or not to allow caching of scripts. • On: No-cache/no-store headers for scripts are not added. • Off: No-cache/no-store headers for scripts are added. The default value is **off**.
allowica on|off
When running Citrix Metaframe using a web client, caching must be allowed. This setting turns off the no-cache headers for ICA files. • On: No-cache/no-store headers for ICA files are not added. • Off:No-cache/no-store headers for ICA files are added. The default value is **on**.
cmsie on|off
Specifies how the virtual SSL server handles the Microsoft Internet Explorer (MSIE) session termination bug workaround. Valid options for the **cmsie** command are:

Command Syntax and Usage
• On: The VPN Gateway closes Windows MSIE SSL sessions with a TCP FIN but without an SSL shutdown. This circumvents the MSIE SSL session termination bug. • Off: The virtual SSL server will always use the FIN (finish) TCP flag to decide when to terminate a client connection. The default value for the **cmsie** setting is **on**.
maxrcount <*numerical value*>
Sets the maximum number of requests for single HTTP/1.1 (or HTTP/1.0 keep-alive) sessions. A HTTP/1.1 session can consist of multiple HTTP requests, one after another. This command lets you set a limit to the number of subsequent requests for a given SSL/TCP session. The default value for the **maxrcount** setting is 40.
maxline <*numerical value*>
Sets the maximum length of HTTP headers in a HTTP client connection request. The default value for the **maxline** setting is 8192.
urlobscure <on/off>
on- Enable the URL obfuscation for the backend server connected through portal. Obfuscation is done based on the Base64 encoding and decoding standard. off - Disables the URL obfuscation for the backend server connected through portal. Obfuscation is done based on the Base64 encoding and decoding standard.

/cfg/vpn <id> /server/http/rewrite HTTP Rewrite Configuration

```
[Rewrite Menu]
      rewrite    - Set SSL triggered rewrite
      ciphers    - Set accepted ciphers
      response   - Set source of response
      URI        - Set URI with the weak cipher alert
```

The Rewrite menu is used for enabling and configuring the HTTP rewrite functionality for the portal server.

Table 119: Rewrite Menu Options (/cfg/vpn/server/http/rewrite)

Command Syntax and Usage
rewrite on|off
Enables or disables the rewrite functionality for the portal server. When you enable the rewrite functionality, a customized error message can be sent back to the client's web browser in case the browser is unable to perform the required cipher strength. If the rewrite functionality is not enabled in such a scenario, the client request is simply rejected during the SSL handshake. For more information about

Command Syntax and Usage
how to configure an SSL server to use the rewrite functionality, see the "Configuring the AVG to Rewrite Client Requests" chapter in the *Application Guide for SSL Acceleration*. The default **rewrite** setting is **off.**
ciphers <*cipher list*> Lets you change the cipher list used when the SSL rewrite function is enabled. The default cipher list used when the rewrite function is not enabled corresponds to ALL@STRENGTH. When the rewrite function is enabled, the default rewrite cipher list is HIGH:MEDIUM. If you change the default rewrite cipher list from HIGH:MEDIUM when having the rewrite function enabled, remember that the rewrite cipher strength must always be higher than the cipher strength specified by using the **/cfg/vpn/server/ssl/ciphers** command (where the default cipher list is ALL@STRENGTH) . For more information about supported ciphers and cipher list formats, see Appendix A, Supported Ciphers, in the *User's Guide*.
response iSD|WebServer
Specifies whether the iSD (VPN Gateway) or a web server should handle the response message sent back to the client. When **response** is set to **WebServer,** use the **URI** command to point to a resource on a web server that can provide a customized error message. The default **response** setting is **iSD.**
URI <*IP address and path to web server resource for response message*> Sets the URI pointing to a resource on a WebServer that provides the response message (when **response** is set to **WebServer**).

/cfg/vpn <id> /server/proxymap Proxy Mapping Configuration

```
[Proxy Mapping Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The Proxy Mapping menu is used for mapping domains or hosts on the intranet to an intranet proxy server. When a match is found between the remote user's request and a domain or host listed here, the request is redirected through the proxy server that has been mapped to that domain/host.

Table 120: Proxy Mapping Menu Options (/cfg/vpn/server/proxymap)

Command Syntax and Usage
list

Command Syntax and Usage
Displays all hosts/domains that are added to the configuration. The entries are listed by their respective index number.
del <*host/domain by index number*>
Removes the specified hosts/domains. Use the **list** command to display all added entries.
add <*host or domain*> <*proxy server and port*>

Lets you map a host or domain to an intranet proxy server.
• Host or domain. Enter the desired host or domain, e.g. www.example.com or example.com. Requests to the specified host or domain will be redirected through the specified proxy server. The first matching entry will be used. To match all hosts/domains, enter * (asterisk).
• Proxy server and port, e.g. proxy.example.com:3128.
If the proxy server requires authentication, you can create a custom single-sign on header using the **ssoheaders** command.
Example 1: Single sign-on header for a proxy server requiring static credentials:
`Proxy-Authorization: Basic <base64:user:password>`
Replace *user* and *password* with the required credentials.
Example 2: Single sign-on header for proxy servers requiring specific user credentials:
`Proxy-Authorization: Basic <base64:<var:user>:<var:password>>`
The <*var:user*> and <*var:password*> variables expand to the logged in VPN user's credentials.
For instructions on how to create custom single-sign on headers, see the **ssoheaders** command on /cfg/vpn <id> /aaa/ssoheaders Single-Sign-On Headers Configuration on page 244.

insert <*index number to insert at*> <*host/domain to add*>
Assigns a specific index number to the host/domain you add. The index number you specify must be in use. Entries with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves a host/domain up or down in the list of configured entries. The index numbers you specify must be in use. To view all entries currently added to the configuration, use the **list** command.

/cfg/vpn <id> /server/portal Portal Server Settings Configuration

```
[Portal Settings Menu]

authentica          - Set User authentication

wipecookie          - Set Wipe all cookies at logout

cookiedb            - Keep the cookie database in VPN gateway

dnrewrite           - Set Rewrite domain name

resetcooki          - Set Re-Set session cookie in each request

domain              - Set cookie domain

persistent          - Set use persistent session cookies
```

The Portal settings menu is for example used for configuring various portal server settings, for example the PortalGuard feature (see the **authentica** command below).

Table 121: Portal Settings Menu Options (/cfg/vpn/server/portal)

Command Syntax and Usage
authentica on|off By setting this command to **off**, the VPN Gateway can make use of the VPN functionality to SSL accelerate an existing intranet web site, for example a portal. The AVG 's AAA system is then bypassed. This feature is also known as the PortalGuard. 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 to include the AVG rewrite prefix. This cannot be achieved with the traditional SSL offload mechanism. The AVG rewrite prefix (boldface) is added to the link properties as shown below: https://vip.example.com /http/inside.example.com/site/file.html To access the intranet web site, the user should enter the Portal IP address or host name. The user will then be redirected to the intranet web site (specified with the **dhost** command) without first having to log in to the Portal. If set to **off**, the **dhost, dscheme** and **dgroup** commands will also be displayed on the Portal settings menu (see below). The default setting is **on**. The **authentica** command is only available if a PortalGuard license has been loaded.

Command Syntax and Usage
Also see the "Configure Portal Guard" chapter in the *Application Guide for VPN*.
wipecookie on|off
• On: The AVG clears all cookies set by the browser when the user logs out/is logged out from the Portal. This also includes the SiteMinder SMSESSION and the ClearTrust CTSESSION cookies. • Off The AVG only clears cookies set by the AVG itself. The default setting is **on**.
resetcooki on|off
By setting this command to **on**, the Portal session cookie will automatically be re-set (that is, set once again) after each HTTP request. This feature is needed for some ActiveX components (for example the Viewer feature in GE PACS) that are designed to wipe all cookies, including the Portal session cookie. The default setting is **off**.
dhost <*backend server host name or IP address and path*>
Sets the backend web server host address and path (if required) when authentication is disabled. Example: **inside.example.com/portal.html**
dscheme http|https
Sets the protocol used to access an intranet web site when authentication is disabled.
dgroup <*group name*>
Sets the default group in which users will be placed when authentication is disabled. Users bypassing the VPN Portal this way will automatically be placed in a default group specified with this command. Prior to disabling authentication, configure the default group using the **/cfg/vpn <id>/group** command and add the desired access rules for that 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.
domain <*domain*>
This command can be used in the special case when several virtual SSL servers are used within the same DNS domain and you wish to eliminate the need for a remote user to log in repeatedly to the different virtual servers. Example: Besides the portal server defined for the web Portal, the example.com domain also includes an http server defined for a password-protected web server. The WWW authentication mode for the http server is set to portal, which is required

Command Syntax and Usage
for this type of single-sign-on to work. (To set the authentication mode for a virtual server, use the **/cfg/ssl/server #/http/auth** command.) The cookie used for client authentication (set by the current SSL server) is sent from the client web browser to all virtual SSL servers within the same DNS domain. The domain to which the cookie is sent should be specified with this command. Example domain: **example.com**
persistent on|off
By setting this command to on, persistent cookies will be used for the Portal login session. This means that the user will still be logged in to the Portal even if the browser is shut down. The default setting is **off.**
cookiedb on|off
By setting this command to on, cookies are stored in the database. The default setting is **on.**
dnrewrite <FQDN>
Portal Domain Name Rewrite feature (Round Robin DNS feature) provides persistent connection within cluster to support inter-cluster load balance service. Persistent connection is provided once the initial contact is made to the AVG, and does not provide inter-cluster session migration on failover. In a deployment scenario, multiple AVG boxes are clustered separately in different locations. To have persistent session with the same cluster, the administrator can configure the secondary DNS name which is associated to each cluster. Once the initial contact is made, the AVG will automatically replace the primary DNS name to secondary DNS name, and then packets will always reach the same cluster, and ensure persistent session within the cluster. Secondary DNS name in each cluster can be configured using the CLI command 'dnrewrite'. This feature does not work without proper DNS configuration.

/cfg/vpn <id> /server/adv Advanced Settings Configuration

```
[Advanced Settings Menu]
traflog    - UDP syslog Traffic Log menu
sslconnect - SSL connect menu
```

The Advanced Settings menu includes commands for accessing the UDP Syslog Traffic Log menu and the SSL Connect Settings menu.

Table 122: Advanced Settings Menu Options (/cfg/vpn/server/adv)

Command Syntax and Usage
traflog Displays the Traffic Log Settings menu. To view menu options, see /cfg/vpn <id>/server/adv/traflog Traffic Logging on page 269.
sslconnect Displays the SSL Connect Settings menu. To view menu options, see /cfg/vpn <id> /server/adv/sslconnect SSL Connection Configuration on page 271.

/cfg/vpn <id>/server/adv/traflog Traffic Logging

```
[Traffic Log Settings Menu]
      protocol   - Set syslog protocol
      sysloghost - Set syslog host IP
      udpport    - Set syslog portnumber
      priority   - Set syslog priority
      facility   - Set syslog facility
      ena        - Enable traffic UDP syslog logging
      dis        - Disable traffic UDP syslog logging
```

The Traffic Log Settings menu is used for configuring a syslog server, to which UDP syslog messages for all HTTP requests handled by the portal server can be sent. Enabling traffic logging through syslog messages will generate a substantial amount of network traffic, and also place additional CPU load on each AVG device in the cluster. Besides, syslog servers are not generally intended for this type of log messages, and the syslog server might therefore not be able to cope with the amount of syslog messages generated within a cluster of multiple AVG devices. In environments where traffic logging must be performed on the SSL terminating device itself due to laws or regulations, traffic logging through syslog messages can be used. It can also be used temporarily for debugging purposes. This setting will generate traffic; therefore it is recommended that you set up syslog on the backend server if possible.

The traffic logging performed by backend web servers can be enhanced by configuring the VPN Gateway to add certain HTTP headers. For more information about available extra HTTP headers, see the HTTP Settings menu on /cfg/ssl/server <id>/http HTTP Settings Configuration on page 99.

Below is an example of a syslog message generated on an AVG device: `Mar 8 14:14:33 192.168.128.24 <ISD-SSL>: 192.168.128.189 TLSv1/SSLv3 DES-CBC3-SHA "GET / HTTP/1.0".`

Table 123: Traffic Log Settings Menu Options (/cfg/vpn/server/adv/traflog)

Command Syntax and Usage
protocol *bsd|ietf* Specifies the syslog message format. Valid options are as follows:

Command Syntax and Usage
• bsd: Syslog message appears in bsd format. The IP and facility information must be provided. • ietf: Syslog message appears in ietf format. The IP and facility information is not required. The default message format is **bsd**.
sysloghost <*IP address of syslog server*>
Specifies the IP address of the syslog server to which syslog messages will be sent using a UDP (User Datagram Protocol) connection.
udpport <*UDP port number of syslog server*>
Specifies the UDP port number of the syslog server. The default UDP syslog server port number is set to 514.
priority debug|info|notice
Configures the priority level of syslog messages that are sent. Valid priority levels, listed from low to high, are: • **debug:** Messages that contain information mainly of use only for debugging purposes. • **info:** Informational messages. • **notice:** Conditions that are not error conditions, but should possibly be handled specially. The default priority level is set to **info.**
facility auth|authpriv|daemon|local0-7
Configures the facility parameter of syslog messages. The facility parameter is used to specify what type of program is logging the message. This lets the configuration file specify that messages from different facilities will be handled differently. The default facility parameter is set to **local4.**
ena
Enables traffic logging through syslog messages to the specified syslog server.
dis
Disables traffic logging through syslog messages to the specified syslog server. Traffic logging through syslog messages is disabled by default.

/cfg/vpn <id> /server/adv/sslconnect SSL Connection Configuration

```
[SSL Connect Settings Menu]
      protocol   - Set protocol version
      cert       - Set client certificate
      ciphers    - Set accepted ciphers for ssl connect
      verify     - Verify server menu
```

The SSL Connect Settings menu is used for configuring the SSL protocol, the preferred cipher list, and client authentication for SSL connections between the VPN Gateway(s) and the backend servers.

Table 124: SSL Connect Settings Menu Options (/cfg/vpn/server/adv/sslconnect)

Command Syntax and Usage
protocol ssl2|ssl3|ssl23|tls1|tls11|tls12 Specifies the protocol the virtual SSL server should propose when establishing an SSL session with an SSL-enabled backend server. Valid options are as follows: • **ssl2:** Propose using only SSL 2.0. • **ssl3:** Propose using SSL 3.0. • **ssl23:** Propose using any of SSL 2.0, SSL 3.0, or TLS 1.0. • **tls1:** Propose using only TLS 1.0. • **tls11:** Only accept TLS 1.1. • **tls12:** Only accept TLS 1.2. The default protocol value is **ssl23.**
cert <*client certificate by index number*> Specifies which client certificate the selected virtual SSL server should present to the backend servers, in case the SSL software on the backend servers is configured to require a client certificate. Client authentication is typically very seldom used for SSL connections between the VPN Gateways and the backend servers, as the client is known in these circumstances. To view basic information about available certificates, use the **/info/certs** command. To generate a client certificate, see the "Generating Client Certificates" section in the "Certificates and Client Authentication" chapter in the *User's Guide*.
ciphers <*cipher list format*> Specifies the list of preferred ciphers. This information is sent to the backend servers during the SSL handshake. The default cipher list corresponds to `ALL:-EXPORT:-LOW!ADH:-SSLv2` , which should be appropriate in most cases. The default cipher list provides for using lighter encryption algorithms between the

Command Syntax and Usage
VPN Gateways and the backend servers than what is normally used between Internet clients and the VPN Gateways. This is desirable mainly in terms of SSL performance. Since both the VPN Gateways and the backend servers typically are behind a firewall in physically secured premises, using lighter encryption algorithms on this network segment should not compromise the overall security. If you change the default list of preferred ciphers, make sure the specified ciphers are included in the backend servers' list of preferred ciphers as the SSL connection will otherwise be refused. For more information about supported ciphers and cipher list formats, see Appendix A, Supported Ciphers, in the *User's Guide*.
verify
Displays the SSL Connect Verify Settings menu. To view menu options, see /cfg/ssl/server <id> /adv /sslconnect/verify SSL Connect Verify Configuration on page 135.

/cfg/vpn <id> /server/adv/sslconnect /verify SSL Connect Verify Configuration

```
[SSL Connect Verify Settings Menu]
      verify     - Set certificate verification level
      commonname - Set server common name
      cacerts    - Set list of accepted signers of server's certificate
```

The SSL Connect Verify Settings menu is used for configuring the desired certificate verification level when back end servers are authenticated. The menu is also used to specify the common name of backend servers, as well as setting the CA certificates used for backend server authentication.

Table 125: SSL Connect Settings Menu Options (/cfg/vpn/server/adv/sslconnect)

Command Syntax and Usage
verify none|require Specifies the authentication level to use when establishing an SSL connection towards a backend server. Valid options are as follows: • None: No server certificate is required. • Require: The server must present a valid certificate in order for the selected virtual SSL server to establish a session. The default value is **none**.
commonname <*common name of backend web server*>
Specifies the common name used in the backend server's server certificate. To establish an SSL session, the common name you specify must match the common name found in the certificate used by the backend server(s).

Command Syntax and Usage
The common name found in the server certificate normally corresponds to the name of the web server as it appears in the URL used by Internet clients when accessing the web server. Do not include the protocol specifier (`http://`) or any port numbers or pathnames in the common name. Wildcards (such as * or ?) and IP address are not allowed.
cacerts <*CA certificate by index number*>
Specifies which of the available CA certificates to use for backend server authentication. To view basic information about all certificates, use the **/info/certs** command. To add a new CA certificate, see the "Adding certificates to the AVG " section in the "Certificates and Client Authentication" chapter in the *User's Guide*. When specifying more than one certificate, use commas to separate the corresponding index number: Example: 1,2,5

/cfg/vpn <id>/l2tp Layer 2 Tunneling Protocol Configuration

```
[L2tp Menu]
      ena        - Enable L2tp
      dis        - Disable L2tp
      quick      - Quick L2tp setup wizard
      ikeprof    - IKE profile
      utunprof   - User tunnel profile
      cacerts    - Set list of accepted signers of remote end certificate
      cert       - Set our server certificate
      secret     - Set shared secret
      authorder  - Set authorder
      groupmatch - Set Enable group matching
```

Layer 2 Tunneling Protocol (L2TP) acts as a data link layer protocol for tunneling network traffic between two peers over an existing network or Internet. Layer 2 Tunneling Protocol acts as a Layer 5 protocol and uses the registered User Datagram Protocol (UDP) port 1701. The L2TP packet including payload and L2TP header, is sent within a UDP datagram. It carries Point-to-Point Protocol (PPP) sessions within the L2TP tunnel. The IPsec provides confidentiality, authentication, and integrity to the L2TP packets. The L2TP/IPsec is combination of these two protocols.

Table 126: L2TP Menu Options (/cfg/vpn/l2tp)

Command Syntax and Usage
ena Enables L2TP on the VPN Gateway.
dis Disables L2TP on the VPN Gateway.
quick Lets you run the Quick L2TP setup wizard for enabling L2TP access in few steps.

Command Syntax and Usage
Note: If `/cfg/vpn #/hostippool` is set to **`false`** , and no **`/cfg/vpn #/ippool`** is configured, then **`cfg/vpn #/l2tp/quick`** prompts for these three extra configuration: `Lower IP address in pool range: Upper IP address in pool range: Primary DNS server:`
`ikeprof`
Displays the IKE Profile Menu. For more information about options, see /cfg/vpn <id>/l2tp/ikeprof <id> IKE Profile Configuration on page 275.
`utunprof`
Displays the User Tunnel Profile Menu. For more information about options, see /cfg/vpn <id>/l2tp/utunprof User Tunnel Profile Configuration on page 281.
`cacerts` *<certificate number 1-1500>*
The cacerts command lists the accepted Certificate Authority (CA) certificates. The CA certificates are used to verify client certificates for user tunnels and server certificates for branch office tunnels. The CA certificate must exist on the VPN Gateway. The CA certificates are added either through cut-and-paste, or through TFTP/FTP/SCP/SFTP from a remote host. Both actions are performed from the Certificate menu. To get an overview over available certificates, enter the **`/info/certs`** command. When specifying more than one certificate, use commas to separate the corresponding index numbers. For example, enter 1,2,5. **Note:** If you are using one of the available certificates to generate your own client certificates, specify it as a CA certificate to successfully authenticate clients. For more information about client authentication, see *Avaya VPN Gateway User's Guide*.
`cert` *<certificate index number>*
Specifies which server certificate must be sent to authenticate the VPN Gateway to the L2TP VPN client (for user tunnels) or to a remote endpoint (branch office tunnel). • L2TP user tunnels: used when the user connects with the L2TP/IPsec VPN client. This command is used only if the VPN clients use client certificates to authenticate the VPN Gateway. The server certificate must exist on the VPN Gateway. For more information about available certificates, enter the **`/info/certs`** command. For more information about adding a new certificate, see *Avaya VPN Gateway User's Guide*.
`secret <shared secret>`
Displays the current secret value. You can also change the shared secret.

Command Syntax and Usage
authorder
Displays the current authentication order. You can also change the authentication order. Default authentication order is: Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAP v1), Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (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
groupmatch true|false
Specifies whether to enable or disable the group match for the group authentication option. Valid options are as follows: • true: Matches the groups returned for the user authentication. • false: Places the user in the group used for the group session. Default value is **true**.

/cfg/vpn <id>/l2tp/ikeprof <id> IKE Profile Configuration

```
[IKE Profile 1 Menu]
      name       - Set IKE profile name
      del        - Remove IKE Profile
      enc        - Encryption mask menu
      dh         - Diffie-Hellman group mask menu
      pfs        - Enable Perfect Forward Secrecy
      icp        - Enable Initial Contact Payload
      vendorid   - Enable Vendor Id Transmission
      rekeytime  - Set rekey time limit
      rekeytraf  - Set rekey traffic limit
      retransmit - Set ISAKMP retransmit interval
      maxretrans - Set ISAKMP max attempts retransmits
      replaywins - Set replay window size
      nat        - Set ESP UDP NAT detect
      deadpeer   - Dead peer menu
```

Use the IKE Profile Menu to configure Internet Key Exchange (IKE) profile. You can configure and map different IKE profiles to different user tunnel profiles.

Table 127: IKE Profile Menu options (/cfg/vpn/l2tp/ikeprof)

Command Syntax and Usage
name Sets the name of the IKE profile. This name is referenced in the user tunnel profile. For more information, see /cfg/vpn <id>/l2tp/utunprof User Tunnel Profile Configuration on page 281.

Command Syntax and Usage
del
Deletes the currently selected IKE profile.
enc
Displays the Encryption Menu. For more information about options, see /cfg/vpn <id>/l2tp/ikeprof <id>/enc IKE Profile Encryption on page 278.
dh
Displays the Diffie-Hellman Group Menu. For more information about options, see cfg/vpn <id>/l2tp/ikeprof <id>/dh Diffie-Hellman Group Configuration on page 279.
pfs on|off
Enables or disables the Perfect Forward Secrecy (PFS) feature. When PFS is enabled, keys are not derived from previous keys. This ensures even if one key is compromised the subsequent keys are not compromised. The default value is **off**.
icp on|off
Enables Initial Contact Payload (ICP).
vendorid on|off
Specify whether or not to pass a unique and vendor-defined constant to the responding side. The AVG uses the constant to identify and recognize remote instances of an Internet Security Association and Key Management Protocol (ISAKMP) implementation. Reception of a familiar Vendor ID payload allows an implementation to make use of payload numbers from 128 to 255 for vendor-specific extensions. • on: The Vendor ID is sent to the responding side when the AVG is initiating the connection (typically in a branch office tunnel configuration). If the Vendor ID is not recognized by the responding side, the connection is managed according to the standard ISAKMP protocol. • off: The Vendor ID attribute is not sent to the responding side. You can use this setting if the appliance at the responder side does not understand the Vendor ID attribute and the connections are dropped. If vendorid is set to Off, the connection is managed according to the standard ISAKMP protocol. When the AVG is responding, the Vendor ID is sent back if the initiating side sends a Vendor ID, regardless of the vendorid setting. The default value is **on**.
rekeytime <*maximum time in seconds, minutes or hours*>
Sets the maximum lifetime of the single session key. The setting controls how often new session keys are exchanged between the client and the VPN Gateway. 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.

Command Syntax and Usage
The default value is 8h (8 hours). The maximum setting is 23h59m59s (23 hours, 59 minutes and 59 seconds). A setting of 0s (0 seconds) disables the service.
rekeytraf <*traffic in Kbytes*>
Sets the maximum traffic allowed before new session keys are exchanged between the client and the VPN Gateway. You can also choose this option instead of **rekeytime** option. The default value is 0. It disables the service.
retransmit
Sets the time interval after which the IKE packet is assumed to be lost and is retransmitted.
maxretrans
Sets the maximum number retransmissions. This is the number of times that the client retransmits a keepalive packet to the VPN Gateway to check for connectivity.
replaywins
Provides a way to define the accepted range of sequence numbers. By default, the sequence number is incremented while handling calls for the sender. This sequence number is used for antireplay and the service is effective only if the receiver checks the sequence number. The default value is 0. It disables the antireplay service.
nat
Lets you select settings option for NAT detection. Valid options are as follows: • disabled: Does not encapsulate the L2TP packets within UDP, even if a NAT device is detected on the way. This option is used if the NAT devices are L2TP aware or if there are no NAT devices. • auto: Forces the L2TP SA to encapsulate the L2TP packets within the UDP whenever a NAT device is detected even if the NAT device is L2TP aware. • ipsec_capable: This option is used when both IPsec aware and non-IPsec aware NAT devices exist within the network environment. An IPsec forwarding subsystem is informed to check whether traffic is received on this IPsec SA for the preconfigured interval: - If traffic is received: indicates NAT device on the network path is IPsec aware and no further action is required. - If no traffic is received: Indicates NAT device is not forwarding the IPsec traffic and UDP encapsulation is required. The IPsec forwarding subsystem sends a rekey initiation to IKE for a new IPsec SA to establish IPsec packets encapsulation within UDP. • 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

Command Syntax and Usage
encapsulated in the UDP port. A non ESP marker header separates IKE traffic from IPsec traffic on the UDP port. The default value is **disabled**.
deadpeer
Displays the Dead Peer Menu. For more information about options, see /cfg/vpn <id>/l2tp/ikeprof <id>/deadpeer IKE Profile Dead Peer Configuration on page 280.

/cfg/vpn <id>/l2tp/ikeprof <id>/enc IKE Profile Encryption

```
[Encryption Menu]
      hmac_md5   - Set HMAC with MD5
      hmac_sha   - Set HMAC with SHA
      null_md5   - Set NULL with MD5
      null_sha   - Set NULL with SHA
      des_md5    - Set DES with MD5
      des_sha    - Set DES with SHA
      3des_md5   - Set 3DES with MD5
      3des_sha   - Set 3DES with SHA
      aes_128_sh - Set 128 bits AES with SHA
      aes_256_sh - Set 256 bits AES with SHA
```

Use the Encryption Menu to set the required encryption parameters for the current IKE profile.

Table 128: Encryption Menu options (/cfg/vpn <id>/l2tp/ikeprof <id>/enc)

Command Syntax and Usage
hmac_md5 on|off Enables or disables the Hash Message Authentication Code (HMAC) with Message-Digest algorithm 5 (MD5) encryption. The default value is **off**.
hmac_sha on|off Enables or disables HMAC with SHA encryption. The default value is **off**.
null_md5 on|off Enables or disables NULL with MD5 encryption. The default value is **off**.
null_sha on|off Enables or disables null with SHA encryption. The default value is **off**.
des_md5 on|off

Command Syntax and Usage
Enables or disables DES with MD5 encryption. The default value is **off**.
des_sha on|off Enables or disables DES with SHA encryption. The default value is **off**.
3des_md5 on|off Enables or disables 3DES with MD5 encryption. The default value is **off**.
3des_sha on|off Enables or disables 3DES with SHA encryption. The default value is **on**.
aes_128_sh on|off Enables or disables 128 bits AES with SHA encryption. The default value is **off**.
aes_256_sh on|off Enables or disables 256 bits AES with SHA encryption. The default value is **off**.

cfg/vpn <id>/l2tp/ikeprof <id>/dh Diffie-Hellman Group Configuration

```
[Diffie-Hellman Group Menu]
      dh1         - Set Diffie-Hellman group 1 with DES
      dh2         - Set Diffie-Hellman group 2 with 3DES
      dh5         - Set Diffie-Hellman group 5 with 128 bit AES
      dh2_aes128 - Set Diffie-Hellman group 2 with 128 bit AES
      dh5_aes256 - Set Diffie-Hellman group 5 with 256 bit AES
```

Use the Diffie-Hellman Group Menu to enable or disable the desired Diffie-Hellman group setting for the current IKE profile.

Note:

When configuring an IKE profile for a branch office tunnel, you can enable only one of the above options.

Table 129: Diffie-Hellman Group Menu options (/cfg/vpn/l2tp/ikeprof/dh)

Command Syntax and Usage
dh1 on|off Enables or disables the Diffie-Hellman group 1 option with DES. The default value is **off**.

Command Syntax and Usage
dh2 on|off
Enables or disables the Diffie-Hellman group 2 option with 3DES. The default value is **on**.
dh5 on|off
Enables or disables the Diffie-Hellman group 5 option with 128 bit AES. The default value is **off**.
dh2_aes128 on|off
Enables or disables the Diffie-Hellman group 2 option with 128 bit AES. The default value is **off**
dh2_aes256 on|off
Enables or disables the Diffie-Hellman group 5 option with 256 bit AES. The default value is **off**

/cfg/vpn <id>/l2tp/ikeprof <id>/deadpeer IKE Profile Dead Peer Configuration

```
[Dead Peer Menu]
      ena        - Enable dead peer detection
      dis        - Disable dead peer detection
      interval   - Set detect interval
      retransmit - Set max retransmissions
```

Use the Dead Peer Menu to configure detection of tunnel failure due to lost connectivity.

If traffic is not received from the client on the L2TP SA and if the VPN Gateway does not receive any keepalive messages from the client during the time frame set as the dead peer detect interval (multiplied with the configured number of retransmissions), the VPN Gateway assumes that client connectivity is lost and the tunnel is brought down.

Table 130: Dead Peer Menu options (/cfg/vpn/l2tp/ikeprof/deadpeer)

Command Syntax and Usage
ena
Enables dead peer detection. Dead peer detection is enabled by default.
dis
Disables dead peer detection. Dead peer detection is enabled by default.
interval <*value in seconds*>
Sets the time to wait after a period of no traffic before checking if a keepalive message is received from the L2TP client. The default value is 3m20s (3 minutes and 20 seconds).

Command Syntax and Usage
retransmit
Sets the maximum number of times for the VPN Gateway to check if a keepalive message is received from the L2TP client. The interval between the retransmissions is set with the **interval** command. The default value is 2.

/cfg/vpn <id>/l2tp/utunprof User Tunnel Profile Configuration

```
[User Tunnel Profile 1 Menu]
      name       - Set User tunnel profile name
      ikeprof    - Set IKE profile for this tunnel
      del        - Remove User Tunnel Profile
```

Use the User Tunnel Profile Menu to make the desired settings for a specific user tunnel profile. After you create user tunnel profile, you must reference in a user access group. Remote users who are members of this group, use the settings made for the referenced user tunnel profile when connecting to the intranet through L2TP.

Table 131: User Tunnel Profile Menu options (/cfg/vpn/l2tp/utunprof)

Command Syntax and Usage
name Sets the name of the user tunnel profile. After creating the name, refer the name in the group when members use the current user tunnel profile in their L2TP connections. To reference the user tunnel profile in a group, use the **/cfg/vpn <id>/aaa/group #/l2tp/utunnel** command.
ikeprof *<reference to name of IKE profile>* Lets you reference a previously created IKE profile. Group members using the current user tunnel profile can use all the settings made in the referenced IKE profile when establishing an L2TP connection to the VPN Gateway.
del Deletes the current user tunnel profile.

cfg/vpn <id>/l2tp/ikeprof <id>/icp Initial Contact Payload Configuration

Use the ICP command to enable or disable the desired Initial Contact Payload setting for the current IKE profile.

Enable Initial Contact Payload (on/off)

Table 132: Initial Contact Payload options (/cfg/vpn/l2tp/ikeprof/icp)

Command Syntax and Usage
(on/off) Enables or disables Initial Contact Payload. The default value is **off**.

/cfg/vpn <id>/ipsec IPsec Configuration

```
[IPsec Menu]
      ena         - Enable IPsec
      dis         - Disable IPsec
      quick       - Quick IPsec setup wizard
      sys         - IPsec System menu
      ikeprof     - IKE profile
      utunprof    - User tunnel profile
      botunprof   - Branch Office Tunnel Profile
      cacerts     - Set list of accepted signers of remote end certificate
      cert        - Set our server certificate
      groupmatch  - Set Enable group matching
      groupbind   - Set Enable RADIUS group binding
```

The IPsec menu is used to configure the VPN Gateway to support IPsec-based user tunnels and branch office tunnels.

Note:

The IPsec menu is not available if the VPN Gateway software is run on the ASA 310 or ASA 410 hardware platforms.

Table 133: IPsec Menu Options (/cfg/vpn/ipsec)

Command Syntax and Usage
ena Enables IPsec on the VPN Gateway.
dis Disables IPsec on the VPN Gateway.
quick Lets you run the Quick IPsec setup wizard for enabling IPsec access in a few steps.

Command Syntax and Usage
Note: If **/cfg/vpn #/hostippool** is set to **false** , and no **/cfg/vpn #/ippool** is configured, then **cfg/vpn #/ipsec/quick** prompts for these three extra configuration: `Lower IP address in pool range: Upper IP address in pool range: Primary DNS server:`
sys Displays IPsec system menu. To view menu options, see /cfg/vpn <id>/ipsec/sys <id>IPsec system configuration on page 285.
ikeprof Displays the IKE Profile menu. To view menu options, see /cfg/vpn <id>/ipsec/ikeprof <id> IKE Profile Configuration on page 286.
utunprof Displays the User Tunnel Profile menu. To view menu options, see /cfg/vpn <id> /ipsec/utunprof User Tunnel Profile Configuration on page 293.
botunprof Displays the Branch Office Tunnel Profile menu. To view menu options, see /cfg/vpn <id> /ipsec/botunprof Branch Office Tunnel Profile Configuration on page 302.
cacerts <*certificate index number*> For IPsec user tunnels (user connects with IPsec VPN client), this command need only be used if VPN clients use client certificates to authenticate to the VPN Gateway. For IPsec branch office tunnels, this command need only be used if the remote endpoint uses a server certificate to authenticate to the VPN Gateway (as opposed to shared secret). The **cacerts** command lets you list accepted CA certificates. The CA certificates is used to verify client certificates for user tunnels and server certificates for branch office tunnels. The CA certificate must exist on the VPN Gateway. CA certificates are added either through cut-and-paste, or through TFTP/FTP/SCP/SFTP from a remote host. Both actions are performed from the Certificate menu. To get an overview over available certificates, enter the **/info/certs** command. When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5 To clear all specified CA certificates, press ENTER when asked to enter the certificate numbers, then answer yes to the question if you want to clear the list. **Note:** If you are using one of the available certificates to generate your own client certificates, you must specify it as a CA certificate to successfully authenticate clients. For more information on client authentication, see the section

Command Syntax and Usage
"Configuring a Virtual SSL Server for Client Authentication" in the "Certificates and Client Authentication" chapter in the *User's Guide*.
cert <*certificate index number*> For IPsec user tunnels (user connects with IPsec VPN client), this command need only be used if VPN clients use client certificates to authenticate to the VPN Gateway. For IPsec branch office tunnels, this command need only be used if the remote endpoint uses a server certificate to authenticate to the VPN Gateway (as opposed to shared secret). The **cert** command specifies which server certificate should be sent to authenticate the VPN Gateway to an IPsec VPN client (for user tunnels) or to a remote endpoint (for branch office tun. The server certificate must exist on the VPN Gateway. To view basic information about available certificates, use the **/info/certs** command. To add a new certificate, see the "Adding Certificates to the AVG " section in the "Certificates and Client Authentication" chapter in the *User's Guide*.
groupmatch <true/false> Specifies whether to enable or disable the group match for the group authentication option. The default value is true, which matches the groups returned for the user authentication. When false, user will be placed on the group that is used for the group session. Default value is true.
groupbind <on/off> Specifies whether to enable or disable the RADIUS group binding option. The default value is disabled.

cfg/vpn id/ipsec/groupbind

```
[IPsec Menu]
     groupbind - Set Enable RADIUS group binding
```

Specifies whether to enable or disable the RADIUS group binding option. The default value is disabled, granting an IP:sec user access depending on the groupmatch option and the user's group returned by RADIUS. In this case, the user is assigned to the user's group returned by RADIUS. In cases where an empty group attribute is returned, the user is assigned to the IPsec's Group ID.

Table 134: Groupbind Menu options (cfg/vpn id/ipsec/groupbind)

Command Syntax and Usage
groupbind <status> Sets the Groupbind status as enabled or disabled.

/cfg/vpn <id>/ipsec/sys <id>IPsec system configuration

```
[IPsec System Menu]
      failover    - IPsec Failover
      nat-t       - NAT Traversal
```

This menu shows the IPsec system menu options.

Table 135: IPsec system configuration Options (/cfg/vpn<id>/ipsec/sys <id>)

Command Syntax and Usage
failover Displays the IPsec failover configuration. To view menu options, see /cfg/vpn <id>/ipsec/sys <id>/failover on page 285.
nat-t Displays the NAT traversal menu. To view menu options, see /cfg/vpn <id>/ipsec/sys <id>/nat-t NAT Traversal Menu on page 286.

/cfg/vpn <id>/ipsec/sys <id>/failover

```
[IPsec Failover Menu]
      primary     - Set Primary failover address
      secondary   - Set Secondary failover address
      tertiary    - Set Tertiary failover address
```

Use the IPsec Failover Menu to configure the primary, secondary, and tertiary failover address.

Table 136: IPsec Failover Menu options (/cfg/vpn <id>/ipsec/sys <id>/failover)

Command Syntax Usage
primary Sets the primary IPsec failover address.
secondary Sets the secondary IPsec failover address.
tertiary

Command Syntax Usage
Sets the tertiary IPsec failover address.

/cfg/vpn <id>/ipsec/sys <id>/nat-t NAT Traversal Menu

```
[NAT Traversal Menu]
      udpport    - Set UDP port
      portswitch - Client IKE source port switching
      ena        - Enable NAT Traversal
      dis        - Disable NAT Traversal
```

The following table shows the menu options of the NAT traversal command.

Table 137: IPsec NAT Traversal/cfg/vpn <id>/ipsec/sys <id>/nat-t

Command Syntax Usage
udport
Sets the UDP port.
portswitch on|off
Sets the client IKE source port switching. The default value is off.
ena
Enables NAT traversal.
dis
Disables NAT traversal.

/cfg/vpn <id>/ipsec/ikeprof <id> IKE Profile Configuration

```
[IKE Profile 1 Menu]
      name       - Set IKE profile name
      del        - Remove IKE Profile
      enc        - Encryption mask menu
      dh         - Diffie-Hellman group mask menu
      pfs        - Enable Perfect Forward Secrecy
      icp        - Enable Initial Contact Payload
      vendorid   - Enable Vendor Id Transmission
      rekeytime  - Set rekey time limit
      rekeytraf  - Set rekey traffic limit
      retransmit - Set ISAKMP retransmit interval
      maxretrans - Set ISAKMP max attempts retransmits
      replaywins - Set replay window size
      nat        - Set ESP UDP NAT detect
      deadpeer   - Dead peer menu
```

The IKE Profile Menu is used to configure the required settings for the IKE (Internet Key Exchange) profile. If needed, several different IKE profiles can be configured and mapped to different user tunnel profiles.

Table 138: IKE Profile Menu options (/cfg/vpn/ipsec/ikeprof)

Command Syntax and Usage
name
Sets the name of the IKE profile. This name should later be referenced in the desired user tunnel profile (see /cfg/vpn <id> /ipsec/utunprof User Tunnel Profile Configuration on page 293).
del
Deletes the currently selected IKE profile.
enc
Displays the Encryption mask menu. To view menu options, see /cfg/vpn <id> /ipsec/ikeprof <id> /enc IKE Profile Encryption on page 289.
dh
Displays the Diffie-Hellman group menu. To view menu options, see /cfg/vpn <id>/ipsec/ikeprof <id> /dh Diffie-Hellman Group Configuration on page 290.
pfs on|off
Enables/disables 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 **on**.
icp on|off
Enables Initial Contact Payload (ICP). he default value is **off**.
vendorid on|off
Lets you specify whether or not to pass a unique, vendor-defined constant to the responding side. The constant is used by the AVG to identify and recognize remote instances of an ISAKMP implementation. Reception of a familiar Vendor ID payload allows an implementation to make use of payload numbers 128-255 for vendor-specific extensions. • On: The Vendor ID is sent to the responding side when the AVG is initiating the connection (typically in a branch office tunnel configuration). If the Vendor ID is not recognized by the responding side, the connection will be managed according to the standard ISAKMP protocol. • Off: The Vendor ID attribute is not sent to the responding side. This setting can be used if the appliance at the responder side does not understand the Vendor ID attribute, in which case it will drop the connection. By setting **vendorid** to **off**, the connection is managed according to the standard ISAKMP protocol. When the AVG is responding, the Vendor ID is sent back if the initiating side has sent a Vendor ID, regardless of the **vendorid** setting. The default value is **on**.

Command Syntax and Usage
rekeytime <*maximum time in seconds, minutes or hours*>
Sets the maximum lifetime of the single session key. The setting controls how often new session keys are exchanged between the client and the VPN Gateway. 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 0s (0 seconds) disables the service.
rekeytraf <*traffic in Kbytes*>
Sets the maximum traffic allowed before new session keys are exchanged between the client and the VPN Gateway. If desired, you can choose this option instead of the rekeytime option (see above). The default value is 0, which disables the service.
retransmit
Sets the time interval after which the IKE packet is assumed to be lost and is retransmitted.
maxretrans
Sets the maximum number retransmissions. This is the number of times that the client retransmits a keepalive packet to the VPN Gateway to check for connectivity.
replaywins
Provides a way to define the accepted range of sequence numbers. By default, the sequence number is incremented while handling calls for the sender. This sequence number is used for antireplay and the service is effective only if the receiver checks the sequence number. The default value is 0, which disables the antireplay service.
nat
Displays the NAT (Network Address Translation) Menu. For more information about options, see /cfg/vpn <id> /ipsec/ikeprof <id> /nat IKE Profile NAT Configuration on page 291.
deadpeer
Displays the Dead Peer Menu. For more information about options, see /cfg/vpn <id>/ipsec/ikeprof <id>/deadpeer IKE Profile Dead Peer Configuration on page 292.

/cfg/vpn <id> /ipsec/ikeprof <id> /enc IKE Profile Encryption

```
[Encryption Menu]
      hmac_md5   - Set HMAC with MD5
      hmac_sha   - Set HMAC with SHA
      null_md5   - Set NULL with MD5
      null_sha   - Set NULL with SHA
      des_md5    - Set DES with MD5
      des_sha    - Set DES with SHA
      3des_md5   - Set 3DES with MD5
      3des_sha   - Set 3DES with SHA
      aes_128_sh - Set 128 bits AES with SHA
      aes_256_sh - Set 256 bits AES with SHA
```

The Encryption Menu is used to set the required encryption parameters for the current IKE profile.

Table 139: Encryption Mask Menu options (/cfg/vpn/ipsec/ikeprof/enc)

Command Syntax and Usage
hmac_md5 on|off Enables or disables HMAC with MD5 encryption. The default value is **off**.
hmac_sha on|off Enables or disables HMAC with SHA encryption. The default value is **off**.
null_md5 on|off Enables or disables NULL with MD5 encryption. The default value is **off**.
null_sha on|off Enables or disables NULL with SHA encryption. The default value is **off**.
des_md5 on|off Enables or disables DES with MD5 encryption. The default value is **off**.
des_sha on|off Enables or disables DES with SHA encryption. The default value is **off**.
3des_md5 on|off Enables or disables 3DES with MD5 encryption. The default value is **off**.

Command Syntax and Usage
3des_sha on|off
Enables or disables 3DES with SHA encryption. The default value is **on**.
aes_128_sh on|off
Enables or disables 128 bits AES with SHA encryption. The default value is **off**.
aes_256_sh on|off
Enables or disables 256 bits AES with SHA encryption. The default value is **off**.

/cfg/vpn <id>/ipsec/ikeprof <id> /dh Diffie-Hellman Group Configuration

```
[Diffie-Hellman Group Menu]
      dh1         - Set Diffie-Hellman group 1 with DES
      dh2         - Set Diffie-Hellman group 2 with 3DES
      dh5         - Set Diffie-Hellman group 5 with 128 bit AES
      dh2_aes128 - Set Diffie-Hellman group 2 with 128 bit AES
      dh5_aes256 - Set Diffie-Hellman group 5 with 256 bit AES
```

The Diffie-Hellman group menu is used to enable/disable the desired Diffie-Hellman group setting for the current IKE profile.

Note:

When configuring an IKE profile for a branch office tunnel, only one of the above options can be enabled.

Table 140: Diffie-Hellman Group Menu Options (/cfg/vpn/ipsec/ikeprof/dh)

Command Syntax and Usage
dh1 on|off Enables/disables the Diffie-Hellman group 1 option with DES. The default value is **off.**
dh2 on|off Enables/disables the Diffie-Hellman group 2 option with 3DES. The default value is **on.**
dh5 on|off Enables/disables the Diffie-Hellman group 5 option with 128 bit AES. The default value is **off**.

Command Syntax and Usage
dh2_aes128 on|off
Enables/disables the Diffie-Hellman group 2 option with 128 bit AES. The default value is **off**.
dh2_aes256 on|off
Enables/disables the Diffie-Hellman group 5 option with 256 bit AES. The default value is **off**.

/cfg/vpn <id> /ipsec/ikeprof <id> /nat IKE Profile NAT Configuration

```
[NAT Menu]
      natdetect  - Set ESP UDP NAT detect
      timeout    - Set detect timeout
      keepalive  - Set keepalive timeout
```

NAT (Network Address Translation) devices on the network path between the client PC and the VPN Gateway may or may not be IPsec aware. IPsec aware NAT devices can handle IPsec traffic but if the NAT device is not IPsec aware, the client PC and the VPN Gateway can negotiate to encapsulate the IPsec packets within UDP (that is, the same as NAT traversal in this document).

The NAT menu is used to configure how NAT device detection and packet encapsulation should be managed by the VPN Gateway.

Table 141: NAT Menu Options (/cfg/vpn/ipsec/ikeprof/nat)

Command Syntax and Usage
natdetect disabled|auto|ipsec_capable
Lets you make the desired setting for NAT detection. • **disabled.** Sets the IPsec SA to not encapsulate the IPsec packets within UDP, even if a NAT device is detected on the way. Used if the NAT devices are IPsec aware or if there are no NAT devices. • **auto.** Forces the IPsec SA to encapsulate the IPsec packets within UDP whenever a NAT device has been detected – even if the NAT device is IPsec aware. • **ipsec_capable.** Should be used if both IPsec aware and non IPsec aware NAT devices exist within the network environment. An IPsec forwarding subsystem is informed to check whether any traffic is received on this IPsec SA for the preconfigured interval: - If traffic is received: This is an indication that the NAT device on the network path is IPsec aware and no further action is required. - If no traffic is received: This indicates that the NAT device is not forwarding the IPsec traffic and UDP encapsulation is required. The IPsec forwarding

Command Syntax and Usage
subsystem sends a rekey initiation to IKE indicating that a new IPsec SA should be established with IPsec packets encapsulation within UDP. The default value is **disabled**.
timeout <*value in seconds*>
Sets the timeout value for NAT detection when **ipsec_capable** is selected (see above). The default value is 30 seconds.
keepalive <*value in seconds*>
Sets the minimum NAT keepalive interval. This interval is used by the client to trigger transmission of NAT keepalive messages when UDP encapsulation is used. The default value is 18 seconds.

/cfg/vpn <id>/ipsec/ikeprof <id>/deadpeer IKE Profile Dead Peer Configuration

```
[Dead Peer Menu]
      ena        - Enable dead peer detection
      dis        - Disable dead peer detection
      interval   - Set detect interval
      retransmit - Set max retransmissions
```

The Dead Peer menu is used to configure detection of tunnel failure due to lost connectivity.

If there is no traffic received from the client on the IPsec SA and if the VPN Gateway does not 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.

Table 142: Dead Peer Menu Options (/cfg/vpn/ipsec/ikeprof/deadpeer)

Command Syntax and Usage
ena Enables dead peer detection. Dead peer detection is enabled by default.
dis Disables dead peer detection. Dead peer detection is enabled by default.
interval <*value in seconds*>
Sets the time to wait after a period of no traffic before checking if a keep alive message has been received from the IPsec client.

Command Syntax and Usage
The default value is 3m20s (3 minutes and 20 seconds).
retransmit Sets the maximum number of times for the VPN Gateway to check if a keep alive message has been received from the IPsec client. The interval between the retransmissions is set with the **interval** command (see above). The default value is 2.

/cfg/vpn <id> /ipsec/utunprof User Tunnel Profile Configuration

```
[User Tunnel Profile 1 Menu]
      name       - Set User tunnel profile name
      ikeprof    - Set IKE profile for this tunnel
      del        - Remove User Tunnel Profile
```

The User Tunnel Profile menu is used to make the desired settings for a specific user tunnel profile. When created, the user tunnel profile should be referenced in a user access group. Remote users who are members of this group will all use the settings made for the referenced user tunnel profile when connecting to the intranet through IPsec.

Table 143: User Tunnel Profile Menu Options (/cfg/vpn/ipsec/utunprof)

Command Syntax and Usage
name Sets the name of the user tunnel profile. This name should be referenced in the group whose members should use the current user tunnel profile in their IPsec connections. To reference the user tunnel profile in a group, use the **/cfg/vpn <id>/aaa/group #/ipsec/utunnel** command.
ikeprof *<reference to name of IKE profile>* Lets you reference a previously created IKE profile. Group members using the current user tunnel profile will make use of all the settings made in the referenced IKE profile when establishing an IPsec connection to the VPN Gateway.
del Deletes the current user tunnel profile.
auto Displays the Auto menu. To view menu options, see /cfg/vpn <id> /ipsec/utunprof <id> /auto Auto Connect Configuration on page 295.
splittun disabled|enabled|enabled_inverse| enabled_inverse_local|enabled_inverse_portal

Command Syntax and Usage
Lets you set the desired split tunnel mode. Split tunneling allows client data to travel either through a tunnel to the VPN Gateway or directly to the Internet. All IPsec client traffic is tunneled through the VPN Gateway by default. Split tunneling lets you configure specific network routes that are downloaded to the client. Only these network routes are then tunneled; any other traffic goes to the local network interface. Split tunneling allows the remote user to print locally, for example, even while tunneled to the VPN Gateway. • **disabled.** Tunnels all IPsec client traffic to the VPN Gateway but does not allow SSL connectivity to the Portal after the tunnel is established. • **enabled.** Tunnels IPsec client traffic through the VPN Gateway to specified networks only (see /cfg/vpn <id> /ipsec/utunprof <id> /splitnets Split Networks Configuration on page 298). All other client traffic goes through the client's normal network interface. SSL connectivity to the Portal is allowed. • **enabled_inverse.** Client traffic is not tunneled to the specified networks (see /cfg/vpn <id> /ipsec/utunprof <id> /splitnets Split Networks Configuration on page 298), that is, goes through the client's normal network interface. All other IPsec client traffic is tunneled through the VPN Gateway. SSL connectivity is allowed if the Portal IP is in a specified network. • **enabled_inverse_local.** IPsec client traffic is not tunneled to directly connected networks. All other IPsec client traffic is tunneled through the VPN Gateway. SSL connectivity to the Portal after the tunnel is established will not be allowed. • **enabled_inverse_portal.** Tunnels all IPsec client traffic to the VPN Gateway and allows SSL connectivity to the Portal after the tunnel is established. The default value is **enabled_inverse_portal**.
splitnets Displays the Split Networks Menu. For more information about options, see /cfg/vpn <id> /ipsec/utunprof <id> /splitnets Split Networks Configuration on page 298.
mobility Displays the Mobility Menu. For more information about options, see /cfg/vpn <id>/ipsec/utunprof <id>/mobility Contivity Client Mobility Configuration on page 299.
banner Lets you enter a text string of your own choice to customize the logon banner for the Avaya VPN client (formerly Contivity). The banner appears at the top of the IPsec VPN client upon logon.
usebanner on|off Enables or disables display of the banner configured with the **banner** command. The default value is **off**.

Command Syntax and Usage
ddnsreg Enables client Dynamic DNS registration. The default value is disabled.
client Displays the Client PC menu. To view menu options, see /cfg/vpn <id> /ipsec/utunprof <id> /client Client PC Control Configuration on page 299.
policies Displays the Client policy rules menu. To view menu options, see /cfg/vpn <id> /ipsec/utunprof <id> /policies Client Policy Configuration on page 300.

/cfg/vpn <id> /ipsec/utunprof <id> /auto Auto Connect Configuration

```
[Auto Menu]
      autoconnmo - Set client auto connect mode
      domains    - Auto connect domains menu
      networklis - Auto connect network menu
```

The Auto menu includes commands to configure the auto connect feature, enabling remote Avaya VPN clients to connect their IPsec tunnel sessions in a single step.

Example: The remote user clicks a web link to a page on the private internal network. This first starts their ISP connection, then makes the tunnel connection to the gateway, and finally makes the connection to the requested destination.

Table 144: Auto Menu Options (/cfg/vpn/ipsec/utunprof/auto)

Command Syntax and Usage
autoconnmo spec_net|any_net Sets the desired client auto connect mode. • **spec_net.** When the client successfully connects to the VPN Gateway, a list of networks and domains that trigger the auto connect feature is downloaded to the client. This list, which is stored in the client 's registry, is used to determine whether a tunnel connection should automatically be started when one is not already active. Use the **domains** and **networklis** commands to specify the desired domains and networks. • **any_net.** A tunnel connection to the VPN Gateway is automatically created, regardless of which network or domain the remote user tries to access.
domains

Command Syntax and Usage
Displays the Auto Connect Domains menu. To view menu options, see /cfg/vpn <id> /ipsec/utunprof <id> /auto/domains Auto Connect Domains Configuration on page 296.
networklis
Displays the Auto Connect Network List menu. To view menu options, see /cfg/vpn <id> /ipsec/utunprof <id> /auto/networklis Auto Connect Network List Configuration on page 297.

/cfg/vpn <id> /ipsec/utunprof <id> /auto/domains Auto Connect Domains Configuration

```
[Auto Connect Domains Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The Auto Connect Domains menu is used to specify the domains to trigger the auto connect feature. To limit the auto connect feature to be triggered by requests to specific networks, proceed to the Auto Connect Network List menu (see next page) without adding any domains on this menu.

Table 145: Auto Connect Domains Menu Options (/cfg/vpn/ipsec/utunprof/auto/domains)

Command Syntax and Usage
list Displays all domains that are added to the current user tunnel profile. The domains are listed by their respective index number.
del <*domain by index number*> Removes the specified domain. Use the **list** command to display the index numbers of all added domains.
add <*host name or domain name*> Adds a host or domain, e.g. www.example.com or example.com. As soon as the remote user tries to access a resource residing on the specified host or in the specified domain, an IPsec tunnel is set up to the VPN Gateway.
insert <*index number to insert at*> <*domain to add*> Assigns a specific index number to the domain you add. The index number you specify must be in use. Domains with an index number higher than (and including) the one you specify will have their current index number incremented by 1.

Command Syntax and Usage
move *<index number to move> <destination index number>*
Moves a domain up or down in the list of configured domains. The index numbers you specify must be in use. To view all domains currently added to the system configuration, use the **list** command.

/cfg/vpn <id> /ipsec/utunprof <id> /auto/networklis Auto Connect Network List Configuration

```
[Auto Connect Network List Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The Auto Connect Network List menu is used to specify the networks to trigger the auto connect feature.

Table 146: Auto Connect Network List Menu Options (/cfg/vpn/ipsec/utunprof/auto/networklis)

Command Syntax and Usage
list Displays all networks that are added to the current user tunnel profile. The networks are listed by their respective index number.
del *<network by index number>*
Removes the specified network. Use the **list** command to display the index numbers of all added networks.
add *<network IP address> <network mask>*
Adds a network to the configuration. • Network IP address, e.g. 10.2.3.4 • Network mask, e.g. 24 (=255.255.255.0).
insert *<index number to insert at> <network to add>*
Assigns a specific index number to the network you add. The index number you specify must be in use. Networks with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move *<index number to move> <destination index number>*
Moves a network up or down in the list of configured networks. The index numbers you specify must be in use. To view all networks currently added to the system configuration, use the **list** command.

/cfg/vpn <id> /ipsec/utunprof <id> /splitnets Split Networks Configuration

```
[Split Networks Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The Split Networks menu lets you add network addresses to be used in split tunnel mode. Configured network addresses are loaded to the IPsec client application when an IPsec tunnel has been established.

In **enabled** mode (see the **splittun** command on /cfg/vpn <id> /ipsec/utunprof User Tunnel Profile Configuration on page 293), only these network routes are tunneled – any other traffic goes to the local PC interface. In enabled_inverse mode, all traffic except these routes are tunneled. In enabled_inverse_local or enabled_inverse_portal mode, the configured network addresses are ignored.

Table 147: Split Networks Menu Options (/cfg/vpn/ipsec/utunprof/splitnets)

Command Syntax and Usage
list Displays all networks that are added to the current user tunnel profile. The networks are listed by their respective index number.
del *<network by index number>*
Removes the specified networks. Use the `list` command to display the index numbers of all added networks.
add *<network IP address> <network mask>*
Adds a network to the configuration. • Network IP address, e.g. 10.2.3.4 • Network mask, for example 24 (=255.255.255.0).
insert *<index number to insert at> <network to add>*
Assigns a specific index number to the network you add. The index number you specify must be in use. Networks with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move *<index number to move> <destination index number>*
Moves a network up or down in the list of configured networks. The index numbers you specify must be in use. To view all networks currently added to the system configuration, use the **list** command.

/cfg/vpn <id>/ipsec/utunprof <id>/mobility Contivity Client Mobility Configuration

```
[Mobility Menu]
      enable     - Enable Contivity client mobility
      maxroamtim - Set max roaming time
      handsfree  - Enable handsfree
      persisttim - Set persistent time
```

Table 148: Contivity Client Mobility Configuration Menu Options (/cfg/vpn/ipsec/utunprof/mobility)

Command Syntax and Usage
enable on|off Enables Contivity Client mobility.
maxroamtim <*value in seconds*> Lets you set maximum roaming time in seconds. The default value is <need info>.
handsfree on|off Lets you to enable or disable handsfree.
persisttim <value in seconds> Lets you set the persistence time in seconds. The default value is <need info>.

/cfg/vpn <id> /ipsec/utunprof <id> /client Client PC Control Configuration

```
[Client PC Menu]
      scrsavepwd - Require client screen saver password
      time       - Set screen saver activation time
      storepwd   - Allow client to store password
```

The Client PC menu includes commands to manage password security on the client PC.

Table 149: Client PC Control Menu Options (/cfg/vpn/ipsec/utunprof/client)

Command Syntax and Usage
scrsavepwd on|off • On: Screen saver password required. Security feature that forces the client to use a password in association with a screen saver. If the user leaves the system and is connected to a tunnel, the system gets locked out of the tunnel once the

Command Syntax and Usage
screen saver kicks in. The end user would enable this feature from the Start > Settings > Control Panel > Display > Screen Saver > Password Protected. • Off: Screen saver password not required. The default value is **off**.
time <*value in seconds*>
This setting is used together with the `scrsavepwd` command. See preceding command for settings. It defines the maximum time before the client's screen saver is activated. The value on the Client PC can be changed from the Start > Settings > Control Panel > Display > Screen Saver > Wait. The default value is 300 seconds.
storepwd on|off
• On: Allows client systems to save the logon password in its password list. • Off: Requires that the remote user enters the password each time he requests authentication and access to an IPsec tunnel. The default value is **on**.

/cfg/vpn <id> /ipsec/utunprof <id> /policies Client Policy Configuration

```
[Client Policy Rules Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

Client policies help prevent potential security violations that could occur when the split tunneling feature is used.

By defining client policies, you can determine which network applications and associated protocols and ports a remote user can have active on his workstation while tunneled.

Table 150: Client Policy Rules Menu Options (/cfg/vpn/ipsec/utunprof/policies)

Command Syntax and Usage
list Displays all client policy rules that are added to the current user tunnel profile. The rules are listed by their respective index number.
del <*client policy rule by index number*> Removes the specified policy rules. Use the **list** command to display the index numbers of all added policy rules.

Command Syntax and Usage
add <*tcp/udp*> <*port number*> <*client/server*>
Adds a policy rule to the configuration. • TCP or UDP. Specifies the protocol used by the application. • Port number. Specifies the port used by the application. 0 means any port. • Client or server. Specifies the type of application, that is, client or server.
insert <*index number to insert at*> <*policy rule to add*>
Assigns a specific index number to the policy rule you add. The index number you specify must be in use. Policy rules with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves a policy rule up or down in the list of configured policy rules. The index numbers you specify must be in use. To view all policy rules currently added to the system configuration, use the **list** command.

cfg/vpn id/ipsec/utunprof<id>/ddnsreg

```
[ddnsreg Menu]
     on   off
     Turn on/off DNS registration
```

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

The administrator can configure whether the client will send this type of messages or not. When connecting to the VPN Gateway, the AVC receives the value of this option and will act accordingly. The default value is enabled, providing behavior as in earlier releases. When the feature is disabled, the DDNS registration message will not be sent by the client.

Table 151: DNS Registration option Menu options (cfg/vpn id/ipsec/utunprof<id>/ddnsreg)

Command Syntax and Usage
ddnsreg [on|off]
Sets the dynamic DNS registration as on or off.

/cfg/vpn <id> /ipsec/botunprof Branch Office Tunnel Profile Configuration

```
[BO Tunnel Profile 1 Menu]
      name       - Set BO tunnel profile name
      del        - Remove BO Tunnel Profile
      ikeprof    - Set IKE profile for this BO tunnel
      vip        - Set the VIP to use as local endpoint for BO tunnel
      remote     - Set Remote endpoint
      group      - Set The AAA group to use for authorization rules
      authtype   - Set Authentication type
      nailedup   - Enable Nailed up tunnel
      sharedsecr - Set Shared secret
      certoid    - Set Remote Cert OID
      remoteid   - Set Remote Identity
      ripannounc - Set RIPv2 announcement of remote networks
      remotenets - List networks behind remote BO end
      localnets  - List local (private) networks
      reset      - Reset BO tunnel
      ena        - Enable BO tunnel
      dis        - Disable BO tunnel
```

The Branch Office Tunnel Profile menu is used to configure the required parameters for setting up a secure IPsec-based branch office tunnel, for example between a main office and a branch office. Several branch office tunnels can be created per VPN. The branch office tunnel will use all encryption settings defined for a previously created IKE profile except the NAT settings.

For more information about configuration examples, see *Application Guide for VPN*.

Table 152: Branch Office Tunnel Profile Menu Options (/cfg/vpn/ipsec/botunprof)

Command Syntax and Usage
name Sets the name of the branch office tunnel profile. This name is mainly for your own reference.
del Deletes the current branch office tunnel profile.
ikeprof *<reference to name of IKE profile>* Lets you reference a previously created IKE profile. Packets coming through the user tunnel will be subject to the encryption settings made in the referenced IKE profile.
vip *<IP address>* Sets the local endpoint public IP address. This is the Portal IP address of the VPN from which the branch office tunnel should be set up. Press TAB to view available Portal IP addresses. The Portal IP address is configured with the **/cfg/vpn <id>/ips** command. For more information, see /cfg/vpn <id> VPN Menu on page 146.

Command Syntax and Usage
remote <*IP address*>
Sets the remote endpoint public IP address. This the IP address of the branch office to which the tunnel should be set up. For example, to set up a branch office tunnel to a specific VPN (as defined on a VPN Gateway at the branch office) the remote IP address must be the Portal IP address of that specific VPN.
group <*user access group*>
Lets you reference a previously defined user access group. The authorization rules of that group will be applied to packets coming out of the branch office tunnel, for example granting or denying access to specific ports and protocols in the branch office networks. Press TAB to view available user access groups. To configure a user access group, use the **/cfg/vpn <id>/aaa/group** command. For more information, see /cfg/vpn <id> /aaa/group <id> Group Configuration on page 226.
authtype sharedsecret|cert
Lets you select the authentication mechanism to be used to authenticate to the other branch office endpoint. • sharedsecret: Sets the authentication mechanism to shared secret. Use the sharedsecr command to enter the shared secret to be used by the branch office tunnel profile. This shared secret should match the shared secret specified at the other branch office endpoint. • cert: Sets the authentication mechanism to certificate. Then use the certoid command to specify which OID value to be extracted from the remote endpoint's server certificate and used for authentication. Finally – with the remoteid command, specify a string to match the extracted value against. The default value is **sharedsecret**.
nailedup on|off
Sets the desired branch office tunnel mode. • On: Nailed Up mode. The VPN Gateway always tries to bring up the tunnel, even though there is no traffic. If the AVG fails to bring up the tunnel it will keep on trying until the tunnel is up. • Off: On Demand mode. The VPN Gateway brings up the tunnel only if traffic is detected. The default value is **off**.
sharedsecr <*shared secret*>
Lets you specify the shared secret when **authtype** is set to sharedsecret. This shared secret must match the shared secret specified at the other branch office endpoint. This command can be ignored if authtype is set to cert.

Command Syntax and Usage
certoid <*OID or symbolic name*>
Lets you specify an OID (object identifier) or symbolic name in the remote endpoint's server certificate. The value that corresponds to this OID/symbolic name will be extracted from the certificate and matched against the string specified with remoteid command. Any OID or symbolic name in the server certificate can be specified as **certoid**. Example: **L/localityName (2.5.4.7) = Test** where localityName is the symbolic name, 2.5.4.7 is the OID and Test is the value. To view available symbolic names, OIDs and values for an existing certificate, use the **/cfg/cert #/subject** command. This command can be ignored if **authtype** is set as **sharedsecret**.
remoteid <*string*>
Enter the string to be matched against the value extracted from the remote endpoint's server certificate. This command can be ignored if authtype is set to sharedsecret.
ripannounc on|off|all
• On: Branch office networks are announced on the private side through the RIPv2 protocol. The announcement is made on all interfaces for the relevant VPN except the traffic interface. This setting is required when the cluster consists of several AVGs. • Off: Branch office networks are not announced on the private side. This setting may cause routing problems when the cluster consists of several AVGs. • All: Same as On command but the announcement is made on all interfaces. The default value is **on**.
remotenets
Displays the Remote BO Networks menu. To view menu options, see /cfg/vpn <id> /ipsec/botunprof /remotenets Remote Branch Office Networks on page 305.
localnets
Displays the Local BO Networks menu. To view menu options, see /cfg/vpn <id> /ipsec/botunprof/localnets Local Branch Office Networks on page 306.
reset
Tears down and reinitiates the tunnel, if established. This command is primarily used to get branch office tunnel profile and AAA changes to take effect for the tunnel.
ena
Enables the branch office tunnel. The branch office tunnel is enabled by default.

Command Syntax and Usage
dis
Disables the branch office tunnel. The branch office tunnel is enabled by default.

/cfg/vpn <id> /ipsec/botunprof /remotenets Remote Branch Office Networks

```
[Remote BO Networks Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
      insert      - Insert a new value
      move        - Move a value by number
```

The Remote Branch Office Networks menu lets you list the branch office networks that should be accessible through the branch office tunnel.

Table 153: Remote Branch Office Networks Menu Options (/cfg/vpn/ipsec/botunprof/remotenets)

Command Syntax and Usage
list Lists the currently configured network entries by index number.
del Removes the network entry that is represented by the index number you specify. Use the **list** command to view all entries and related index numbers currently added to the list.
add *<network IP address> <network mask>* Lets you add the network IP address and network mask of a remote branch office network. To add an additional network/mask to the list, simply enter the **add** command once again.
insert Lets you assign a specific index number to the network entry you add. The index number you specify must be in use. Network entries with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move Lets you move a network entry up or down in the list. To view all network entries, use the **list** command.

/cfg/vpn <id> /ipsec/botunprof/localnets Local Branch Office Networks

```
[Local BO Networks Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The Local Branch Office Networks menu lets you list the local networks from which traffic can be sent to the branch office through the secure branch office tunnel.

Table 154: Local Branch Office Networks Menu Options (/cfg/vpn/ipsec/botunprof/localnets)

Command Syntax and Usage
list Lists the currently configured network entries by index number.
del Removes the network entry that is represented by the index number you specify. Use the **list** command to view all entries and related index numbers currently added to the list.
add *<network IP address> <network mask>* Lets you add the network IP address and network mask of a remote branch office network. To allow all local networks to send traffic through the tunnel, specify the network IP address as 0.0.0.0 and the network mask as 0 . To add an additional network/mask to the list, simply enter the **add** command once again.
insert Lets you assign a specific index number to the network entry you add. The index number you specify must be in use. Network entries with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move Lets you move a network entry up or down in the list. To view all network entries, use the **list** command.

/cfg/vpn <id> /ippool <id> IP Pool Configuration

```
[Pool 1 Menu]
      type       - Set pool mechanism
      name       - Set pool name
      lowerip    - Set lower IP in pool range
      upperip    - Set upper IP in pool range
      exclude    - Exclusion list for the IP pool
      netattr    - Pool network attributes menu
      proxyarp   - Set proxy arp on clean side interfaces
      info       - Print alloc info for this Pool
      ena        - Enable pool
      dis        - Disable pool
      del        - Remove Pool
```

The 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 IPsec VPN client (formerly the Contivity 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.

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 with the **`/cfg/vpn <id>/aaa/group <id></ippool`** command, you can create different methods for IP address and network attributes assignment for different user groups. One of the IP pools should be selected as the default IP pool for the VPN, using the **`/cfg/vpn id>/aaa/defippool`** command. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

Table 155: IP Pool Menu Options (/cfg/vpn/ippool)

Command Syntax and Usage
`type local|radius|dhcp` Sets the source for allocation of IP address and network attributes to the IPsec VPN client and the Net Direct client. • **`local:`** Lets you configure an IP address range on the AVG, using the **`lowerip`** and **`upperip`** commands (see below). This range will be used to allocate IP addresses to IPsec and Net Direct client sessions. The network

Command Syntax and Usage
attributes configured under **netattr** (see command below) will be pushed to the client. • **radius:** IP address and network attributes will be retrieved from an external RADIUS server (if configured) when the remote user is authenticated. See the **/cfg/vpn <id>/aaa /auth #/radius/netattr** command. • **dhcp:** IP address and network attributes will be retrieved from an external DHCP server. Also see the **dhcp** command below.
name <*pool name*>
Lets you to specify pool name.
lowerip <*IP address*>
Sets the IP address from and including which the IP range starts. This command is only available if the **type** command (see above) has been set to **local**.
upperip <*IP address*>
Sets the IP address to and including which the IP range ends. This command is only available if the **type** command (see above) has been set to **local**.
exclude
Displays Exclude Menu Configuration. To view menu options, see /cfg/vpn <id>/ippool <id>/exclude Exclude Menu Configuration on page 309. This command is only available if the **type** command (see above) is set to **local**.
dhcp
Displays the DHCP menu. To view menu options, see /cfg/vpn <id> /ippool <id> /dhcp DHCP Configuration on page 310. This command is only available if the **type** command (see above) is set to **dhcp**.
netattr
Displays the Network attributes menu. To view menu options, see /cfg/vpn <id> /ippool <id> /netattr Network Attributes Configuration on page 311.
proxyarp on|off|all
Used for return traffic when the cluster consists of several VPN Gateways and no specific routes are configured. • **on.** The VPN Gateway that handed out the pool IP address for a specific client connection will respond to ARP requests on behalf of the IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets

Command Syntax and Usage
to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. • **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. The default value is **on**.
info

Prints IP allocation information about active VPN tunnels for the current VPN. The information includes configured IP address range, free IP addresses or ranges and currently allocated IP addresses. It also shows which VPN Gateway (iSD) that owns the IP address.
`range  = 10.1.82.100-10.1.82.149`
`free     =`
`franges   =    10.1.82.102-10.1.82.149`
`alloc    =     'isd@a10-1-82-145'  has 10.1.82.100`
`'isd@a10-1-82-148'  has 10.1.82.101`

ena
Enables the IP pool (disabled by default).
dis
Disables the IP pool (disabled by default).
del
Deletes the IP pool.

/cfg/vpn <id>/ippool <id>/exclude Exclude Menu Configuration

```
[Exclude List Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
```

Table 156: Exclude List Menu Options (/cfg/vpn/ippool/exclude)

Command Syntax and Usage
list Lists all the values in the IP pool.
del Deletes the IP pool value.

Command Syntax and Usage
add <ip> [<upperip>]
Lets you add the list of IP addresses that you wish to exclude.

/cfg/vpn <id> /ippool <id> /dhcp DHCP Configuration

```
[DHCP Menu]
servers    - DHCP servers menu
```

The DHCP menu consists of a command to access the DHCP servers menu where DHCP servers can be added or removed.

Note:

To be able to access the DHCP menu, the **/cfg/vpn <id>/ippool <id>/type** command must be set to dhcp (see /cfg/vpn <id> /ippool <id> IP Pool Configuration on page 307).

Table 157: DHCP Menu Options (/cfg/vpn/ippool/dhcp)

Command Syntax and Usage
servers
Displays the DHCP servers menu. To view menu options, see /cfg/vpn <id> /ippool <id> /dhcp/servers DHCP Servers Configuration on page 310.

/cfg/vpn <id> /ippool <id> /dhcp/servers DHCP Servers Configuration

```
[DHCP Servers Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

The DHCP servers menu lets you add one or several external DHCP servers to the configuration.

Table 158: DHCP Servers Menu Options (/cfg/vpn/ippool/dhcp/servers)

Command Syntax and Usage
list Displays all DHCP servers that are added to the configuration. The servers are listed by their respective index number and IP address.
del <*DHCP server by index number*> Removes the specified DHCP server from the configuration. Use the **list** command to display the index numbers of all added servers.
add <*IP address of DHCP server*> Adds a DHCP server to the configuration. Specify the IP address of the DHCP server. The next available index number is automatically assigned by the system.
insert <*index number to insert at*> <*IP address of DHCP server to add*> Assigns a specific index number to the DHCP server you add. The index number you specify must be in use. DHCP servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*> Moves a DHCP server up or down in the list of configured servers. The index numbers you specify must be in use. To view all DHCP servers currently added to the configuration, use the **list** command.

/cfg/vpn <id> /ippool <id> /netattr Network Attributes Configuration

```
[Network Attributes Menu]
      netmask    - Set Netmask for client
      primnbns   - Set Primary NBNS server
      secnbns    - Set Secondary NBNS server
      primdns    - Set Primary DNS server
      secdns     - Set Secondary DNS server
      domainname - Set DNS domain name
```

The Network attributes menu includes commands for example to configure primary and secondary NBNS and DNS servers. The information configured here is pushed to the Avaya VPN client (formerly the Contivity VPN client) or the Net Direct VPN client when assigned to the current IP pool.

The Network attributes menu is primarily intended for IP pools of the **local** type. For IP pools of the **radius** and **dhcp** types, network attributes configured here will be used as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute.

Table 159: Network Attributes Menu Options (/cfg/vpn/ippool/netattr)

Command Syntax and Usage
netmask <*network mask*> Sets the network mask for the client. The network mask should cover the IP address range specified with the **/cfg/vpn <id>/ippool <id>/ lowerip** and **upperip** commands. The default network mask is 255.255.255.0.
primnbns <*IP address*> Sets the IP address of a primary NBNS server (NetBIOS Name Server). Use this command if the 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.
secnbns <*IP address*> Sets the IP address of a secondary NBNS server.
primdns <*IP address*> Sets the IP address of a primary DNS server. Use this command if the 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. The command to use is **/cfg/vpn <id>/adv/dns /servers**. (This option is only possible if a Secure Services Partitioning license is loaded). This server name is used if a default DNS server is specified using **/cfg/sys/dns/servers** command.
secdns <*IP address*> Sets the IP address of a secondary DNS server.
domainname <*domain name*> Lets you specify the name of the domain used while a 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.

/cfg/vpn <id>/hippool Host IP Pool Configuration

```
[Host IP pool 1 Menu]
      name       - Set pool name
      host       - host menu
      proxyarp   - Set proxy arp on clean side interfaces
      info       - Print alloc info for this Pool
      ena        - Enable Host IP Pool
      dis        - Disable Host IP Pool
      del        - Remove Host IP pool
```

You can associate the IP allocated to the clients (Net Direct, IPsec, and L2TP clients) from a pool to 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.

This option is available when host IP pool is enabled using **cfg/vpn <id>/hostippool** command.

Table 160: Portal Menu options (/cfg/vpn/hippool)

Command Syntax and Usage
name Displays current pool name and allows you to change.
host <host number> Displays the Host Menu. For more information about options, see /cfg/vpn <id>/hostippool <id>/host <id> Host Menu on page 314.
proxyarp on|off|all Used for return traffic when the cluster consists of several VPN Gateways and no specific routes are configured. • **on**: The VPN Gateway that handed out the pool IP address for a specific client connection responds to ARP requests on behalf of the IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. • **off**: Return traffic does not reaches its destination unless specific routes are configured. • **all**: Same as **on** but Proxy ARP is used on all interfaces. The default value is **on**.
info Prints IP allocation information about active VPN tunnels for the current VPN. The information includes configured IP address range, free IP addresses or ranges and currently allocated IP addresses. It also shows which VPN Gateway (iSD) that owns the IP address.

Command Syntax and Usage

Following is the output for /cfg/vpn <id>/hippool/info with two host members in a cluster:
>> Main# **cfg/vpn <id>/hippool/info**
`** Host 134.177.220.249`
`range = 10.20.30.1-10.20.30.4`
`free =`
`10.20.30.2`
`10.20.30.3`
`10.20.30.4`
`franges =`
`alloc = (1 allocated IPs)`
`'isd@a134-177-220-249' has 10.20.30.1`
`** Host 134.177.220.65`
`range = 11.11.11.1-11.11.11.3`
`free =`
`11.11.11.1`
`11.11.11.2`
`11.11.11.3`
`franges =`
`alloc = (0 allocated IPs)`

ena
Enables host IP pool. By default, the host IP pool is disabled.
dis
Disables host IP pool. By default, the host IP pool is disabled.
del
Removes host IP pool.

/cfg/vpn <id>/hostippool <id>/host <id> Host Menu

```
[Host 1 Menu]
      ip          - Set IP address
      lowerip     - Set lower IP in pool range
      upperip     - Set upper IP in pool range
      netattr     - Pool network attributes menu
      del         - Remove Host
```

Table 161: Portal Menu Options (/cfg/vpn/hippool/host)

Command Syntax and Usage
ip Allows you to specify host IP address.
lowerip Allows you to specify lower IP address pool range.

Command Syntax and Usage
upperip
Allows you to specify upper IP address pool range.
netattr
Displays Network Attributes menu. To view options, see /cfg/vpn <id>/hippool <id>/host <id>/netattr Network Attributes Configuration on page 315.
del
Removes the host.

/cfg/vpn <id>/hippool <id>/host <id>/netattr Network Attributes Configuration

```
[Network Attributes Menu]
      netmask    - Set Netmask for client
      primnbns   - Set Primary NBNS server
      secnbns    - Set Secondary NBNS server
      primdns    - Set Primary DNS server
      secdns     - Set Secondary DNS server
      domainname - Set DNS domain name
```

Table 162: Portal Menu Options (/cfg/vpn/hippool/host/netattr)

Command Syntax and Usage
netmask <network mask>
Sets the network mask for the client. The network mask must cover the IP address range specified with the **/cfg/vpn <id>/hippool <id>/host/lowerip** and **upperip** commands. The default network mask is 255.255.255.0.
primnbns <IP address>
Sets the IP address of a primary NBNS server (NetBIOS Name Server). Use this command if the VPN client uses a specific NBNS server to contain computer names resolved into IP addresses. NBNS servers provide WINS (Windows Internet Naming Service), which is part of the Microsoft Windows NT server environment.
secnbns <IP address>
Sets the IP address of a secondary NBNS server.
primdns <IP address>
Sets the IP address of a primary DNS server. Use this command if the VPN client uses a specific DNS server to contain domain names resolved into IP addresses.

Command Syntax and Usage
If no (primary or secondary) DNS server is specified here, the DNS server specified for the VPN to which the remote user belongs is used. The command to use is **/cfg/vpn <id>/adv/dns /servers**. (This option is only possible if a Secure Services Partitioning license is loaded.) This server name is used if a default DNS server is specified using **/cfg/sys/dns/servers** command.
secdns <IP address>
Sets the IP address of a secondary DNS server.
domainname <domain name>
Lets you specify the name of the domain used while a tunnel is connected. It ensures that domain lookup operations point to the correct domain. This is important for clients using Microsoft Outlook or Exchange, to ensure mail server is mapped to the correct domain.

/cfg/vpn <id> /portal SSL VPN Portal Configuration

```
[Portal Menu]
      import     - Import banner image gif
      restore    - Restores default Nortel banner
      banner     - Show installed banner file
      redirect   - Set redirect URL
      logintext  - Set static text on login page
      seclogtext - Set static text on second login page
      iconmode   - Set Home tab icon mode
      linktext   - Set static text on link page
      linkurl    - Set url input field on link page
      punblock   - Set add site to popup unblock list
      linkcols   - Set number of columns on home tab
      linkwidth  - Set width of link columns on home tab
      companynam - Set company name used on portal pages
      smbworkgrp - Set default SMB workgroup name
      autojre    - Set silent jre install
      colors     - Portal colors menu
      content    - Portal custom content menu
      faccess    - Full Access menu
      lang       - Portal language menu
      wiper      - Set use ActiveX component for clearing cache
      rsaauto    - Set rsa soft token autofill
      ieclear    - Set use IE ClearAuthCache
      whitelist  - White-list settings menu
      blacklist  - Black-list settings menu
      citrix     - Set Citrix support
      usertype   - VPN User Type based access control menu
      trustsite  - Set automatic trusted zone addition
```

The Portal menu is used to 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 IE cache wiper and configure URL rewrite behaviour.

Table 163: Portal Menu Options (/cfg/vpn/portal)

Command Syntax and Usage
import *<protocol [tftp|ftp|scp|sftp]> <server by host name or IP address> <name of GIF file>* Downloads a banner file in the GIF format from a TFTP/FTP/SCP/SFTP server. When the download is complete and you apply the changes, the current banner image on the Portal web page is replaced. The size of the banner image file should not exceed 16MB. If several VPNs exist, the total size of imported banner image files should not exceed 16MB. **Note:** Users that are currently logged in will not notice the change unless they reload the Portal web page.
restore Restores the default Avaya banner.
banner Displays the file name of the banner image file currently in use.
redirect *<URL, e.g. https://vpn.example.com/ http/inside.example.com>* Sets the URL to which users should automatically be redirected after having authenticated to the Portal. Note that the portal address should be added before the URL, either as is or by using the *<var:portal>* macro. To redirect the user to an internal password-protected site without a second login, enter for example **https://<var:portal>/http/<var:user>:<var:password>@inside.example.com/protected** when prompted for the URL. This requires the user name and password required on the intranet site to be identical with the Portal's user name and password. Note that the user will not be able to access the Portal tabs. To remove a previously entered URL, simply press ENTER when prompted for the URL. 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 a logout link in HTML format might look like: **** Logout from portal
logintext *<text string or HTLM code>* Lets you specify a custom text to be displayed on the Portal Login page, as an ordinary text string or as HTML code. Having entered the **logintext** command, type or paste the desired text. Press ENTER to create a new line and type **...**
seclogtext <text string>

Command Syntax and Usage
Lets you specify the custom text to be displayed on the Portal's second Login page. After entering **seclogtext** command, type or paste the desired text. Press ENTER to create a new line and type **...** to terminate the text entry.
iconmode clean|fancy
Lets you set the desired mode for the Portal's link icons, for example file server links, web server links and port forwarder links. For more information about linksets and links, see /cfg/vpn <id> /linkset <id> Linkset Configuration on page 332. • **clean.** Displays simple icons using a single one color. The color used is color3 (see/cfg/vpn <id> /portal/colors Portal Colors Configuration on page 322). • **fancy.** Displays multi-colored, shaded and animated icons. The default value is **fancy**.
linktext
Sets the static text that is displayed for all SSL VPN users on the Portal's Home tab. The text is displayed preceding the links that are specific for an SSL VPN user, depending on their group membership. The link text can either be typed directly in the CLI, or pasted when prompted. Follow the instructions provided in the CLI when using the **linktext** command. The text can also be interspersed with HTML tags to add formatting elements to the text. You can also use the following macros in the link text: • <*var:user*>: This macro automatically replaces <*var:user*> with the currently logged in SSL VPN user's user name. • <*var:group*>: This macro automatically replaces <*var:group*> with the name of the group in which the currently logged in SSL VPN user is a member. If the user is a member of more than one group, the name of the primary group is used. The first match between a group name defined in the VPN and any group listed in the authentication mechanism that applies to the user is considered the primary group. When searching for a matching group name, the system starts with group ID 1, then continues with group ID 2 and so on until a match is found. The chapter "Customize the Portal" in the *Application Guide for VPN* includes an example of how to configure group-controlled redirection to internal sites by embedding the <var:group> macro in a Java-script.
punblock on|off
Allows you to add website to the popup unblock list. The default value is **off**.
linkurl on|off
Sets the display mode for the Enter URL field on the Portal's Home tab. • **on:** The Enter URL field is displayed. • **off:** The Enter URL field is not displayed.

Command Syntax and Usage
The default value is **on**.
linkcols
Sets the desired number of columns in the link table on the Portal's Home tab. Example: If the number of link columns is set to 4, links 1 to 4 are placed on the first row, links 5-8 on the second row and so on. Additional links are added in sequential order from left to right on the next row. If for example link 2 is deleted, links 3-4 are adjusted left to fill the blank space, link 5 is moved up to the first row and links 6-8 are adjusted left. The default value is 2.
linkwidth auto|0-100%
Sets the width of the link table on the Portal's Home tab. The link table is adjusted to the left on the Home tab's white area. • **auto:** Set number of columns are distributed evenly across the Home tab. • **0-100%:** Determines the amount of space used for the link table. 100% means that the entire white area on the Home tab will accommodate the link table. The default value is 100%.
companynam
Sets your own company name. This name will be displayed instead of "Avaya" on the Portal pages. The company name is displayed as a "tool tip" when hovering the mouse pointer over the Portal banner (logo) and in the browser window's title bar.
smbworkgrp
Lets you specify a default value for Windows workgroup for SMB (Windows file share) servers. The default value is suggested in the [Workgroup] field on the Portal's Files tab and when creating SMB links (see /cfg/vpn <id> /linkset <id> /link <id> /smb SMB Link Configuration on page 336). When the AVG software is first delivered, the default value is **WORKGROUP**.
autojre on|off
Specifies installation of Java Runtime Environment (JRE). • **on**: installs JRE automatically. • **off**: does not install JRE automatically. The default value is **on**.
colors
Displays the Portal Colors Menu. To view menu options, see /cfg/vpn <id> /portal/colors Portal Colors Configuration on page 322.
content

Command Syntax and Usage
Displays the Portal Custom Content Menu. To view menu options, see /cfg/vpn <id> /portal/content Portal Custom Content Configuration on page 323.
faccess
Displays the Full Access menu. To view menu options, see /cfg/vpn <id> /portal/faccess Full Access Configuration on page 324.
lang
Displays the Portal Language menu. To view menu options, see /cfg/vpn <id> /portal/lang Portal Language Configuration on page 326.
wiperon|group|off
• **on:** The remote user will have the option to download the IE cache wiper when logging in to the Portal. If downloaded, the IE cache wiper will clear the cache and browser history when the Portal session is terminated or when the browser is closed. Note that this only applies to HTML pages accessed through the Portal during the secure session. Previously cached content and history entries will not be cleared. The IE cache wiper is only available for users running Internet Explorer. • **group:** Lets you enable/disable the IE cache wiper per user group instead of per VPN. Use the **/cfg/vpn <id>/aaa/group <id>/wiper** command to enable or disable the IE cache wiper on group level. • **off:** The IE cache wiper cannot be downloaded by the user. To allow caching of documents, the **/cfg/vpn <id>/server/http/allowdoc** command can be used. The cache will however not be cleared. The default setting is **on** . **Note:** For best performance, the **allowdoc** command should be set to **off** (default setting) when **wiper** is set to **on**.
rsaauto on|off
Sets RSA soft token autofill. The default value is on.
ieclear on|off
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:** When the user logs out from the Portal, the cache is cleared for all instances of the current IE process. This means that if the user is logged in to another web site, he will be automatically logged out from that site. • **off:** When the user logs out from the Portal, the cache is not cleared until the user closes the browser.

Command Syntax and Usage
Also see the **wiper** setting above. The default value is **on**.
whitelist
Displays the White-list Settings menu. To view menu options, see /cfg/vpn <id> /portal/whitelist White-list settings menu on page 328.
blacklist
Displays the Black-list Settings menu. To view menu options, see /cfg/vpn <id> /portal/blacklist Black-list settings menu on page 330.
citrix on|group|off
Enables/disables support for Portal links to Citrix Metaframe servers. • **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** link type (also see /cfg/vpn <id> /linkset <id> /link <id> /internal Internal Link Configuration on page 371). • **group:** Lets you enable/disable Citrix Metaframe support per user group instead of per VPN. Use the **/cfg/vpn <id>/aaa/group <id>/citrix** command to enable or disable Citrix Metaframe support on group level. • **off:** Links to Citrix Metaframe servers are only supported if the link is created by means of the **custom** port forwarder link type. If Citrix Metaframe links are not used, **off** is the recommended setting, because this saves the AVG from starting the Java applet that supports this feature. **Note:** When **citrix** is set to **on** (on VPN level or group level), the AVG supports rewrite of ICA files only. Other methods are possible but may require configuration changes on the Citrix Metaframe server side. The default value is **off**.
usertype
Displays User Type menu. To view menu options, see /cfg/vpn <id>/portal/usertype User Type Menu on page 331
trustsite on|off
Specifies addition of the VPN portal to the trusted zone. • **on**: adds VPN portal to the trusted zone automatically. • **off**: does not add VPN portal to the trusted zone automatically. The default value is **off**.

/cfg/vpn <id> /portal/colors Portal Colors Configuration

```
[Portal Colors Menu]
      color1     - Set portal color 1
      color2     - Set portal color 2
      color3     - Set portal color 3
      color4     - Set portal color 4
      theme      - Color theme
```

The Portal Colors menu is used to customize the Portal page with respect to colors. Even though the Portal's individual colors can be changed, we recommend using color themes. Also consider how the applied colors fit with the colors of your company logo.

The color code should be entered as a hexadecimal value and is not case-sensitive. For a list of common colors with their corresponding hexadecimal value, see the "Customize the Portal" chapter in the *Application Guide for VPN*.

Note:

Users that are currently logged in will notice the change when they reload the Portal web page.

Table 164: Portal Colors Menu Options (/cfg/vpn/portal/colors)

Command Syntax and Usage
color1 *<#hexadecimal color code>* Refers to the large background area below the tabs. The default value is **#ACCDD5**.
color2 Refers to the background area behind the tab labels. The default value is **#D0E4E9**.
color3 Refers to the active tab, the fields and information area and clean icons. The default value is **#2088A2**.
color4 Refers to non-active tabs. The default value is **#58B2C9**.
themedefault|aqua|apple|jeans|cinnamon|candy Lets you select a color theme for the Portal. The default value is **default**.

/cfg/vpn <id> /portal/content Portal Custom Content Configuration

```
[Portal Custom Content Menu]
      import     - Import content as .zip file
      export     - Export content as zip file
      delete     - Delete all content from portal
      available  - Show available space
      show       - Show custom content directory
      ena        - Enable access to custom content
      dis        - Disable access to custom content
```

The Portal Custom Content menu 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`** link type (see /cfg/vpn <id> /linkset <id> /link <id> /external External Link Configuration on page 370). 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.

Table 165: Portal Custom Content Menu Options (/cfg/vpn/portal/content)

Command Syntax and Usage

`import` *<protocol [tftp|ftp|scp|sftp]> <server host name or IP address> <file name on server> <FTP user name and password>*
 	
Lets you import the desired file or directory structure in .zip format to the Portal from a TFTP/FTP/SCP/SFTP server. The file is saved in the Portal's root directory and is automatically unpacked.
If the content you wish to import to the Portal requires caching on the remote user's machine when executed, create a directory called `avaya_cacheable` . Then store the content in this directory before zipping the files (sub-directories may exist). File and directory names are case sensitive.
Examples of zip file contents:
 	
`noncacheable_content1.html`
`subdir/noncacheable_content2.html`
`avaya_cacheable/mycacheable_content1.html`
`avaya_cacheable/subdir/mycacheable_content2.html`
 	
Also see the **`/cfg/vpn/server/http/allow*`** commands on /cfg/vpn <id> /server/http HTTP Settings Configuration on page 258 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 the existing Portal content, use the export command (see below).

Command Syntax and Usage
export *<protocol [tftp|ftp|scp|sftp]> <server host name or IP address> <file name on server> <FTP user name and password>*
Lets you export an existing zip file from the Portal to a TFTP/FTP/SCP/SFTP server.
delete
Deletes all uploaded content from the Portal.
available
Shows the Portal's available space in kbytes.
show
Enables you to view custom content directory.
ena
Enables access to custom content for the remote user. Disabled by default.
dis
Disables access to custom content for the remote user. Disabled by default.

/cfg/vpn <id> /portal/faccess Full Access Configuration

```
[Full Access Menu]
      ena         - Enable 'Full Access' tab
      dis         - Disable 'Full Access' tab
      ipsecmode   - Set IPSEC Mode
      contip      - Set Contivity IP address
      contid      - Set Contivity group ID
      contpass    - Set Contivity group password
      portalmsg   - Set text in 'Full Access' portal tab
      appletmsg   - Set text in 'Full Access' Applet window
```

The Full Access menu is used to enable display of the Access tab on the Portal. When this tab is displayed, remote users with the Avaya VPN client (formerly the Contivity VPN client) or the Avaya SSL VPN client installed on their local machines can open a connection in transparent mode to the corporate intranet. If neither of the preceding VPN clients are installed or able to connect, the Net Direct VPN client is started (if enabled).

For the Avaya VPN client to be able to connect to an Avaya VPN Router (formerly Contivity), the Full Access menu also lets you configure the required parameters for authentication to the Avaya VPN Router.

When the user clicks the Yes button on the Access tab, a Java applet is downloaded to the remote user's local machine. The applet first checks if the IPsec VPN client is installed and able to connect. If so, the IPsec VPN client is silently activated and instructed to connect to an Avaya VPN Router (in contivity mode) or to the VPN Gateway (in native mode). If not, the

applet goes on to check if the SSL VPN client is installed and able to connect. If the SSL VPN client is not installed or able to connect, the Net Direct VPN client is started (if enabled for the VPN or for the group in which the user is a member).

If neither of the preceding VPN clients are installed or able to connect, intranet resources can only be accessed in clientless mode, that is, through the Portal's tabs.

For a detailed description of the Access tab and the actions involved when a user activates transparent access, see the chapter "The Portal from an End-User Perspective" in the *Application Guide for VPN*.

RSA SecurID is not supported as a means of authenticating to the Avaya VPN Router.

Table 166: Full Access Menu Options (/cfg/vpn/portal/faccess)

Command Syntax and Usage
ena
Enables the Full Access tab on the Portal. Disabled by default.
dis
Disables the Full Access tab on the Portal. Disabled by default.
ipsecmode native|contivity
Sets the desired Full Access mode. • **native:** Instructs the IPsec VPN client to connect to the VPN Gateway. Requires IPsec to be enabled (see /cfg/vpn <id>/ipsec IPsec Configuration on page 282). The **contip, contid** and **contpass** commands (see below) can be ignored. • **contivity:** Instructs the IPsec VPN client to connect to an Avaya VPN Router (formerly Contivity). Requires configuration of VPN Router information (see the following commands).
contip <*IP address*>
Sets the IP address of the Avaya VPN Router.
contid <*group ID*>
Sets the Avaya VPN Router group ID. This is only required if the IPsec VPN client uses group authentication to authenticate to the VPN Router. Once authenticated to the VPN Router with group ID and password, the IPsec VPN client transfers the remote user's user name and password, as provided on the Portal. If the Avaya VPN Router allows user name and password authentication, the VPN client authenticates to the VPN Router using the remote user's user name and password, as provided on the Portal. Contact the VPN Router administrator for more information.

Command Syntax and Usage
contpass *<password>*
Sets the VPN Router group password. This is only required if the IPsec VPN client uses group authentication to authenticate to the VPN Router. Contact the VPN Router administrator for more information.
portalmsg
Lets you enter or paste a custom text to show up on the Full Access tab on the Portal. If no text is entered here, a default text will be displayed on the Full Access tab.
appletmsg
Lets you enter or paste a custom text to show up in the upper section of the Java applet window displayed when a remote user clicks the Yes button on the Portal's Full Access tab. If no text is entered here, a default text will be displayed in the Java applet window.

/cfg/vpn <id> /portal/lang Portal Language Configuration

```
[Portal Language Menu]
      setlang    - Set the language to be used in the portal
      charset    - Print charset in use
      list       - List supported languages
      beconv     - Backend charset conversion handling menu
```

The Portal Language menu is used to set the preferred language for the Portal associated with the currently selected VPN. The portal automatically tries to select the language for the user, based on the default language set in the browser. The user will also be able to switch languages manually.

Table 167: Portal Language Menu Options (/cfg/vpn/portal/lang)

Command Syntax and Usage
setlang *<ISO 639 language code>*
Sets the desired language for Portal button and field labels, screen texts, messages, help texts and so on. Prior to setting the preferred language, the corresponding language definition file must be imported to the configuration. See the Language Support menu on /cfg/lang Language Support Configuration on page 449.
charset
Prints the character set that is currently in use on the Portal.
list

Command Syntax and Usage
Lists the currently supported languages by language code and description.
beconv
Displays the Backend Conversion menu. To view menu options, see /cfg/vpn <id> /portal/lang/beconv Backend Character Set Conversion on page 327.

/cfg/vpn <id> /portal/lang/beconv Backend Character Set Conversion

```
[Backend Conversion Menu]
      add         - Add backend conversion
      del         - Delete backend conversion
      codesets    - Lists all supported backend codesets
      list        - List backend conversion(s)
```

The Backend Conversion menu 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 VPNs 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, configure the AVG to convert the ISO-8859-1 character set to the existing character set for the VPN (that is, SHIFT_JIS) before sending the file list to the browser.

The VPN's existing character set can be checked with the **charset** command (see /cfg/vpn <id> /portal/lang Portal Language Configuration on page 326).

Character set conversion is not required for SMB servers running on Windows 2000 or XP, because they support Unicode natively.

Table 168: Backend Conversion Menu Options (/cfg/vpn/portal/lang/beconv)

Command Syntax and Usage
add <*protocol (smb or ftp)*> <*host*> <*shared network folder (for smb)*> <*character set*>
Adds a backend conversion entry to the configuration. • Protocol. Lets you specify whether to make the conversion for an FTP file server or an SMB (Windows file share) file server. • Host. Lets you specify the backend file server's host name or IP address. • Shared network folder (only for SMB). Lets you limit conversion to a specific file share folder. • Character set. Lets you specify the character set to be converted, for example ISO-8859-1.

Command Syntax and Usage
del
Deletes the backend conversion that corresponds to the index number you specify.
codesets
Lists all character sets that can be used in backend conversion.
list
Lists the currently supported backend conversions by index number.

/cfg/vpn <id> /portal/whitelist White-list settings menu

```
[White-list Settings Menu]
      domains    - Configure white-list domains
      ena        - Enable URL rewrite white-list
      dis        - Disable URL rewrite white-list
```

One of the fundamental features of the VPN Gateway product is the act of rewriting URLs to ensure that traffic is sent through a secure SSL connection, through the AVG. 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. 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 be sent directly to the destination, without passing the AVG.

If unqualified domain names are used (for example inside instead of inside.example.com) the request is always rewritten, even if the domain is not included in the whitelist.

The function is similar to that of the internal link (see /cfg/vpn <id> /linkset <id> /link <id> Link Configuration on page 333), only you cannot add internal links to other web pages than the Portal's Home tab.

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.

Table 169: White-list Settings Menu Options (/cfg/vpn/portal/whitelist)

Command Syntax and Usage
domains
Displays the White-list Domains menu. To view menu options, see /cfg/vpn <id> /portal/whitelist/domains White-list Menu on page 329.

Command Syntax and Usage	
ena	
	Enables the white-list. Continue with specifying whitelist domains. If whitelisting is enabled without specifying whitelist domains, all requests will be sent directly to the destination without being rewritten.
dis	
	Disables the white-list.

/cfg/vpn <id> /portal/whitelist/domains White-list Menu

```
[White-list menu Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
```

The White-list domains menu is used to add domains to the whitelist. Requests for domains listed as whitelist domains will be rewritten with the AVG rewrite prefix (see add command below). All other requests will pass directly to the destination, without passing the AVG.

Table 170: White-list Domains Menu Options (/cfg/vpn/portal/whitelist/domains)

Command Syntax and Usage	
list	
	Lists added whitelist domains by their index number and domain address.
del	
	Removes the domain corresponding to the index number you specify. Use the list command to view all domains and related index numbers currently added to the list.
add	
	Adds a domain name to the whitelist. Example: By entering example.com, all requests for URLs matching the example.com domain will be rewritten to include the AVG rewrite prefix (boldface): https://vpn.example.com /http/www.example.com

/cfg/vpn <id> /portal/blacklist Black-list settings menu

```
[Black-list Settings Menu]
      domains    - Configure black-list domains
      ena        - Enable URL rewrite black-list
      dis        - Disable URL rewrite black-list
```

The blacklist is a list of domains to which requests should not be sent through a secure SSL connection, that is, the URLs should not be rewritten with the AVG rewrite prefix (compare to the whitelist on /cfg/vpn <id> /portal/whitelist White-list settings menu on page 328).

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 whitelist domain and public.example.com as a blacklist domain.

Table 171: Black-list Settings Menu Options (/cfg/vpn/portal/blacklist)

Command Syntax and Usage
domains Displays the Black-list Domains menu. To view menu options, see /cfg/vpn <id> /portal/blacklist /domains Black-list Domains Menu on page 330.
ena Enables the black-list.
dis Disables the black-list.

/cfg/vpn <id> /portal/blacklist /domains Black-list Domains Menu

```
[Black-list menu Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
```

The Black-list domains menu is used to add domains to the black-list. If a remote user clicks a web link whose URL matches a domain in the black-list, the URL will not be rewritten with the AVG rewrite prefix, that is, traffic will not be sent trough a secure SSL connection.

Table 172: Black-list Domains Menu Options (/cfg/vpn/portal/blacklist/domains)

Command Syntax and Usage
list

Command Syntax and Usage
Lists added black-list domains by their index number and domain address.
del
Removes the domain corresponding to the index number you specify. Use the list command to view all domains and related index numbers currently added to the list.
add
Adds a domain name to the black-list. Example: By adding public.example.com as a black-list domain, all requests for URLs matching the public.example.com domain will not be rewritten with the AVG rewrite prefix (see /cfg/vpn <id> /portal/whitelist White-list settings menu on page 328).

/cfg/vpn <id>/portal/usertype User Type Menu

```
[UserType Menu]
      novice      - Access Control for the Novice User
```

Table 173: User Type Menu Options (/cfg/vpn/portal/usertype)

Command Syntax and Usage
Lets you to provide access control on the Home tab (containing group links) and Tools tab. To view menu options, see /cfg/vpn <id>/portal/usertype/ Novice Menu on page 331.

/cfg/vpn <id>/portal/usertype/ Novice Menu

```
[Novice Menu]
      sysinfo     - Set System Information and Bandwidth test menu
```

Table 174: Novice Menu Options (/cfg/vpn/portal/usertype)

Command Syntax and Usage
sysinfo on|off
Displays system information and bandwidth test tool on the Home and Tools tab.

/cfg/vpn <id> /linkset <id> Linkset Configuration

```
[Linkset 1 Menu]
      name       - Set linkset name
      text       - Set linkset text
      autorun    - Set autorun support
      link       - Link menu
      del        - Remove linkset
```

The Linkset menu is used to create a linkset, that is, 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.

Table 175: Linkset Menu Options (/cfg/vpn/linkset)

Command Syntax and Usage
name Lets you enter a name for the current linkset. This name should later be referenced in the desired user groups using the **/cfg/vpn <id>/aaa /group <id>/linkset** command. When you reference a linkset in a group, members of this group will get access to all the links in the linkset. The links are displayed on the Portal's Home tab. If you ran the VPN Quick Setup wizard during the initial setup, the empty linkset `base-links` was created by default as Linkset 1 and mapped to the `trusted` group.
text *<text string or HTLM code>* Lets you enter a heading for the current linkset, as an ordinary text string or as HTML code. The heading will be displayed preceding the links in the linkset on the Portal's Home tab. Configuring a linkset text is optional.
autorun true|false With autorun support enabled, 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. Example: You have configured a port forwarder link to connect to a specific Exchange server and start Microsoft Outlook. As soon as the user enters the Portal, the connection to the Exchange server is automatically set up and Microsoft Outlook is started.
link Displays the Link menu, after you have typed the index number or name of an existing link. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> Link Configuration on page 333. If you type the index number of a new link you will enter a wizard prompting you for the following information:

Command Syntax and Usage	
	• Link text. Enter the clickable link text to be displayed on the Portal's Home tab. • Type of link. Press TAB to view available link types. Then enter the name of the desired link type. For an explanation of each link type, see the Link menu on /cfg/vpn <id> /linkset <id> /link <id> Link Configuration on page 333. When you have entered the link type you will enter the wizard for that particular link type.
del	
	Removes the current linkset.

/cfg/vpn <id> /linkset <id> /link <id> Link Configuration

```
[Link 1 Menu]
move            - Move link
text            - Set link text
type            - Set link type
smb             - SMB settings menu
ftp             - FTP settings menu
forwarder       - Custom port forwarder settings menu
wts             - Window terminal server menu
citrix          - Citrix menu
netdirect       - Net Direct settings menu
terminal        - Terminal settings menu
external        - External settings menu
internal        - Internal settings menu
```

```
iauto           - Iauto settings menu

del             - Remove link
```

The Link menu lets you enter the clickable text that constitutes the link, change link type or delete the link. You can also edit an existing link from here by selecting the corresponding command, internal to edit a previously created link to an internal web page.

All the links that you create under a specific linkset ID will be displayed together on the Portal's Home tab for a user group – if the linkset is mapped to that user group. To map a linkset to a user group, use the **/cfg/vpn <id>/aaa/group <id>/linkset/add**command.

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 user is a member.

Note:

Not all menu items appear at the same time; the `smb, ftp, proxy, ftpproxy, forwarder` (includes `custom, mail, telnet, netdrive, wts` and `outlook), netdirect, wts,citrix, terminal, external, internal` and `iauto` items each appear only when they are selected as the link type.

Linksets can also be mapped to extended profiles. See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of groups, access rules and profiles.

Table 176: Link Menu Options (/cfg/vpn/linkset/link)

Command Syntax and Usage
move *<link number>* Lets you move a link to another position in the linkset. Example: Two Portal links exist as Link 1 and Link 2. To move Link 2 to the top, use the move command and enter 1 as the number to move the link to. Link 2 now becomes Link 1 and Link 1 becomes Link 2.
text Lets you enter the clickable link text to appear on the Portal's Home tab. **Note:** The user will only see the link text, not the URL in the link. It is therefore recommended that you define a descriptive link text that clearly indicates the provided resource.
type *<press TAB following this command to view available link types>* Lets you select the desired link type, for example if you want to change the link type for an existing link. Press TAB following the **type** command to view available

Command Syntax and Usage

link types. After you have selected the desired link type (for example smb), the Link menu will change to include a command corresponding to the selected link type.
Example:
`[Link 1 Menu]`
`move - Move link`
`text - Set link text`
`type - Set link type`
`smb  - SMB settings menu   <--- Selected link type`
`del  - Remove link`
Use the command (**smb** in the preceding example) to enter the Settings menu for the current link type. Then use the **quick** command to run a wizard for the selected link type. For descriptions of the information required by the wizard, see the relevant command below.
If you set the type to **custom, mail, telnet, netdrive, wts** or **outlook**, the **forwarder** command will be displayed in the Link menu. By using the **forwarder** command you will enter a Settings menu specific for the port forwarder type you have selected, e.g. **outlook.**
Note:
When you create a new link (using the **/cfg/vpn <id>/linkset/link command**), you will automatically enter a wizard prompting you for link text and type. The wizard then continues to prompt you for the required data for the selected link type.

smb
Displays the SMB settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /smb SMB Link Configuration on page 336.
ftp
Displays the FTP settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /ftp FTP Link Configuration on page 338.
proxy
Displays the Proxy settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /proxy Proxy Link Configuration on page 339.
ftpproxy
Displays the FTP Proxy menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /ftpproxy FTP Proxy Link Configuration on page 340.
forwarder
Displays the Port Forwarder settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /forwarder <custom> Custom Port Forwarder Link Configuration on page 343.
netdirect

Command Syntax and Usage	
	Displays the Net Direct menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /netdirect Net Direct Link Configuration on page 368.
wts	
	Displays the wts menu. To view menu options, see Table 188: WTS menu (/cfg/vpn <id>/linkset <>id/link/wts) on page 363.
citrix	
	Displays the citrix menu. To view menu options, see Table 189: Citrix menu (/cfg/vpn/linkset/link/Citrix) on page 366.
terminal	
	Displays the Terminal settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /terminal Terminal Link Configuration on page 369.
external	
	Displays the External settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /external External Link Configuration on page 370.
internal	
	Displays the Internal settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /internal Internal Link Configuration on page 371.
iauto	
	Displays the Iauto settings menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /iauto Iauto Link Configuration on page 372.
del	
	Removes the current link from the configuration.

/cfg/vpn <id> /linkset <id> /link <id> /smb SMB Link Configuration

```
[SMB Settings Menu]
quick- Quick SMB link wizard
```

The SMB Settings menu lets you run a quick setup wizard for creating a link to a folder on an SMB (Samba) file server, that is, a Windows file share.

Table 177: SMB Settings Menu Options (/cfg/vpn/linkset/link/smb)

Command Syntax and Usage
quick <*SMB host by IP address or host name*> <*workgroup*> <*name of shared network folder*> <*add as single-sign-on domain*>
Lets you enter a wizard for creating a link to a specific folder on an SMB server. • SMB host. Enter the IP address or host name of the SMB file server, e.g. **10.1.10.1** or **smb.example.com.** Short names can be used, (e.g. **smb**) if **example.com** has been configured as a search domain using the **/cfg/vpn <id>/adv/dns/search** command). • Workgroup (optional). If needed, a Windows workgroup can be specified. To skip this step, press ENTER. • Shared network folder (optional). Enter the path to the desired shared network folder, e.g. **home share/john/manuals**. This folder's content will be listed when the remote user clicks the link. Folder names are not case sensitive and spaces are allowed. When prompted for the path to a shared network folder, you can use these macros in the path: - <*var:user*>This macro expands to the currently logged in SSL VPN user's user name, and thereby provides access to that user's home share folder. Example: **home share/** <*var:user*> - <*var:group*> This macro expands to the name of the group in which the currently logged in user is a member. If the user is a member of more than one group, the name of the primary group is used. The first match between a group name defined in the VPN and any group listed in the authentication mechanism that applies to the user is considered the primary group. When searching for a matching group name, the system starts with applying group ID 1, then continues with group ID 2 and so on until a match is found. The <*var:group*> macro can be used to provide access to a project folder or other folder shared by a group of users. **Note:** Specifying a shared network folder is required for an SMB link to work on a PDA Portal. • Add domain as single-sign-on domain (yes/no). 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 is specified as a single sign-on domain, using the **/cfg/vpn <id>/aaa/ssodomains /add** command or by entering **yes** here. Single sign-on is however always possible if the user name and password is specified in the link, e.g. **user:password@smb.example.com**.

/cfg/vpn <id> /linkset <id> /link <id> /ftp FTP Link Configuration

```
[FTP Settings Menu]
quick- Quick FTP link wizard
```

The FTP Settings menu lets you run a quick setup wizard for creating a link to a directory on an FTP (File Transfer Protocol) file server.

Table 178: FTP Settings Menu Options (/cfg/vpn/linkset/link/ftp)

Command Syntax and Usage
quick *<FTP server by IP address or host name> <initial path> <add as single-sign-on domain>*
Lets you enter a wizard for creating a link to a directory on an FTP server. • FTP host. Enter the IP address or host name of the FTP file server, e.g. **10.1.10.1** or **ftp.example.com.** • Initial path. Enter the path to the desired directory, e.g. **/home/share/john/manuals/.** If an initial path is not specified, the FTP server's root directory is implied. To specify the logged in user's home directory, enter /! as initial path. Note that directory names are case sensitive. Spaces in directory names are however allowed. When prompted for the initial path, you can use the following macros in the path: - *<var:user>* This macro expands to the currently logged in user's user name, and thereby provides access to that user's home directory. Example: **home/share/** *<var:user>* - *<var:group>* This macro expands to the name of the group in which the currently logged in user is a member. If the user is a member of more than one group, the name of the primary group is used. The first match between a group name defined in the VPN and any group listed in the authentication mechanism that applies to the user is considered the primary group. When searching for a matching group name, the system starts with applying group ID 1, then continues with group ID 2 and so on until a match is found. The *<var:group>* macro can for example be used to provide access to a project directory or other directory shared by a group of users. If a shared directory with a name that corresponds to the name of the primary group exists, that directory is displayed for all logged in users who are members of the related group. • Add domain as single-sign-on domain (yes/no). For security reasons, automatic login to the FTP file server (using the Portal login credentials) is only possible if the FTP server's domain name is specified as a single sign-on domain, using the **/cfg/vpn <id>/aaa/ssodomains/add** command or by entering **yes** here. Single sign-on is however always possible if the user name and password is specified in the link, e.g.

Command Syntax and Usage
user:password@ftp.example.com. For anonymous mode, enter **ftp** or **anonymous** before the colon (:) and any text string after the colon.

/cfg/vpn <id> /linkset <id> /link <id> /proxy Proxy Link Configuration

```
[Proxy Settings Menu]
quick- Quick proxy link wizard
```

The Proxy Settings menu lets you run a quick setup wizard for creating an HTTP Proxy link. The HTTP Proxy link is designed to handle proper display of web pages if the remote user has clicked a web link where the HTTP or HTTPS request is embedded in a plug-in (for example in a Flash movie). Without the HTTP Proxy running, such requests might not reach the VPN Gateway.

The HTTP Proxy link lets the user download a Java applet to the client. By reconfiguring the client browser's proxy settings to route all HTTP and HTTPS requests through the Java applet, the traffic will be tunneled through SOCKS (encapsulated in SSL) to the AVG 's proxy server, where it is unpacked and redirected to its destination.

Table 179: Proxy Settings Menu Options (/cfg/vpn/linkset/link/proxy)

Command Syntax and Usage
quick *<update client proxy settings> <open new browser window> <initial URL> <HTTP proxy host and port (optional)> <HTTP proxy user name and password>* Lets you enter a wizard for creating an HTTP proxy link. Instructions on how to reconfigure the client browser's proxy settings is provided in the Java applet window. Note that manual client reconfiguration is not needed if you select to update the client's proxy settings (first option below). • Update client proxy settings. Selecting **yes** means that the client browser's proxy settings are automatically updated when the user clicks the link. Note that this setting only applies to Internet Explorer running on Windows. • Open new browser window. Selecting **yes** means that a new browser window will automatically be opened when the user clicks the **proxy** link. • Initial URL. Sets the start page for the HTTP Proxy session if the link is set to open a new browser window (see the option above). • HTTP Proxy host/port (optional). If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP

Command Syntax and Usage
address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. **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.

/cfg/vpn <id> /linkset <id> /link <id> /ftpproxy FTP Proxy Link Configuration

```
[FTP proxy menu]
quick- Quick FTP proxy link wizard
lhost- Set local host
lport- Set local port
rhost- Set remote host
rport- Set remote port
app  - Set application path
appargs    - Set application arguments
splash     - Set splash text in Applet window
phost- Set proxy host
pport- Set proxy port
puser- Set proxy username
ppass- Set proxy password
debug- Set debug messages
```

The FTP Proxy menu includes commands for creating and editing an FTP proxy link. The FTP proxy link is used to run a native client FTP application (installed on the remote user's client) towards a remote FTP file server, for example on the intranet. When the user clicks the FTP proxy link, one or several SOCKS tunnels (encapsulated in SSL) are created between the user's local machine and the VPN Gateway. The AVG acts as an FTP Proxy and relays data to and from the remote host by setting up sockets to a remote TCP port.

To create an FTP proxy link from scratch, use the **quick** command. To edit specific parts of an existing link, see the other commands on the FTP Proxy menu.

Table 180: FTP Proxy Menu (/cfg/vpn/linkset/link/ftpproxy)

Command Syntax and Usage
quick *<local IP> <local port> <remote FTP server> <remote FTP port> <application path> <application arguments> <text to be displayed in applet window> <HTTP proxy host and port> <HTTP proxy host user name and password>*
Lets you run a wizard for creating an FTP proxy link. The link can be used for running a native FTP client application towards a remote FTP server. If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value, using the **/cfg/vpn <id>/server/tcp/ckeep** command. • Local host IP address. Sets the IP address associated with the client computer, e.g. **127.0.0.1** or any other IP address in the 127.x.y.z range. • Local port. Arbitrary local port number. Ports just preceding 5000 are usually free to use. Port 21 is suggested by default. • Remote FTP server. IP address or host name of the remote FTP file server, e.g. **ftp.example.com**. • Remote FTP port. Port number of the FTP server. Port 21 is suggested by default. • Application path (optional). Defines the application to be started when the user clicks the link. By default, `cmd /c start ftp` is suggested, which means that the FTP session will be run in the command window. Specify the full path to the executable after the prompt, e.g. `C:\Program Files\Application\app.exe`. If the user should start the application manually, use the **app** command (see below) after completing the wizard to clear the application path specification. In this case, user instructions can be provided following the `Paste text...` prompt (see Text below). • Application arguments (optional). Defines the command-line argument to be used by the application, in this case the local host IP address. • Text. Replaces the standard text in the Java applet window, that is, more user-friendly instructions can be supplied. Having entered the text, press ENTER and type three periods (...). Finally press ENTER once again. To keep the standard text (information about host file mappings and opened sockets), type three periods and press ENTER. • HTTP proxy host/port. If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password.
lhost

Command Syntax and Usage
Lets you edit the local host IP address. The local host IP address is the IP address associated with the client computer. The local host IP address can for example be **127.0.0.1** or any other IP address in the 127.x.y.z range. The **lhost** command corresponds to the local host IP address step in the Quick Setup wizard.
lport
Lets you edit the local port number. Ports just preceding 5000 are usually free to use. The **lport** command corresponds to the local port step in the Quick Setup wizard.
rhost
Lets you edit the remote host IP address. The remote host IP address is the IP address associated with the FTP file server. The **rhost** command corresponds to the remote FTP host step in the Quick Setup wizard.
rport
Lets you edit the remote host port number. The remote host port number is the application-specific port number of the application server, for example 21 for FTP traffic. The **rport** command corresponds to the remote FTP port step in the Quick Setup wizard.
app
Lets you specify the application to be started when the user clicks the FTP proxy link. The **app** command corresponds to the application path step in the Quick Setup wizard.
appargs
Lets you specify the argument to the application. The **appargs** command corresponds to the application arguments step in the Quick Setup wizard.
splash
Lets you specify the text to appear in the Java applet window if you want custom user instructions to be displayed. The **splash** command corresponds to the text step in the Quick Setup wizard.
phost
Lets you specify the IP address or domain name of an intermediate intranet HTTP Proxy server, if users are working from a location requiring traffic to pass through such a proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway.

Command Syntax and Usage	
	The **phost** command corresponds to the HTTP proxy host step in the Quick Setup wizard.
pport	
	Lets you specify the port number of an intermediate intranet HTTP Proxy server. The **pport** command corresponds to the HTTP proxy port step in the Quick Setup wizard.
puser	
	If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **puser** command corresponds to the HTTP proxy user name step in the Quick Setup wizard.
ppass	
	If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **ppass** command corresponds to the HTTP proxy password step in the Quick Setup wizard.

/cfg/vpn <id> /linkset <id> /link <id> /forwarder <custom> Custom Port Forwarder Link Configuration

```
[Port forwarder Menu]
quick- Quick port forwarder wizard
tunnel     - Tunnel menu
app  - Set application path
appargs    - Set application arguments
splash     - Set splash text in Applet window
phost- Set proxy host
pport- Set proxy port
puser- Set proxy username
ppass- Set proxy password
```

The Port Forwarder menu includes commands for creating and editing port forwarder links. Port forwarder links are used to run native client applications (installed on the remote user's client) towards a remote server, for example on the intranet. When the user clicks a port forwarder link, one or several SOCKS tunnels (encapsulated in SSL) are created between the user's local machine and the VPN Gateway. The AVG relays data to and from the remote host by setting up sockets to remote TCP or UDP ports.

The Port Forwarder menu looks the same irrespective of the selected port forwarder type (`custom, mail, telnet, netdrive, wts` or `outlook`). The Quick Setup wizard will however ask different questions depending on the selected type.

To edit specific parts of the link, see the other commands on the Port Forwarder menu.

Table 181: Port Forwarder Menu (/cfg/vpn/linkset/link/forwarder)

Command Syntax and Usage
quick (custom) *<traffic mode UDP/TCP> <local IP> <local port> <remote destination host> <remote destination port> <host mapping> <another port forwarder> <application path> <application arguments> <text to be displayed in applet window> <HTTP proxy host and port> <HTTP proxy host user name and password>* Lets you run a wizard for creating a custom port forwarder link. The link can be used for running a native client application towards a remote server. If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value, using the **/cfg/vpn <id>/server/tcp/ckeep** command. • Traffic mode. Lets you specify which network protocol (UDP or TCP) should be used for the connection. • Local host IP address. Sets the IP address associated with the client computer, e.g. **127.0.0.1** or any other IP address in the 127.x.y.z range. • Local port. Arbitrary local port number. Ports just preceding 5000 are usually free to use. • Remote destination host. IP address or host name of the remote application server, e.g. www.example.com. • Remote destination port. Application-specific port number of the application server, e.g. **80** for HTTP traffic. • Host mapping. Can be specified if the user should start the application using this alias, that is, no executable has been specified. This requires the alias to be mentioned in the Java applet text. It also requires the user to have administrator privileges on the client 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. • Yet another port forwarder. Lets you configure yet another tunnel to be set up when the user clicks the link. • Application path (optional). Defines the application to be started (for example explorer.exe) when the user clicks the link. The VPN Gateway must be able to find the executable either through the PATH variable or in the registry (on Windows), that is, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths. If you are in doubt, specify the full path to the executable after the prompt, `e.g. C:\Program Files\Application\app.exe`. If no executable is specified, the user can start the application manually. In this case, user instructions can be provided following the `Paste text...` prompt (see Text below). If **browser** is used as executable, the user's default browser will be started.

Command Syntax and Usage
• Application arguments (optional). Defines the command-line argument to be used by the application, for example http://127.0.0.1:5025 if the executable is `browser` . Note that each application has its own set of arguments. • Text. Replaces the standard text in the Java applet window, that is, more user-friendly instructions can be supplied. Having entered the text, press ENTER and type three periods (...). Finally press ENTER once again. To keep the standard text (information about host file mappings and opened sockets), type three periods and press ENTER. • HTTP proxy host/port. If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. For further examples, see the "Group Links" chapter in the *Application Guide for VPN*.
tunnel
Displays the Tunnel menu where you can edit the tunnel specifics of the current port forwarder link, that is, traffic mode, local host/port, remote host/port and host mapping. The **tunnel** command corresponds to the first five steps in the Quick Setup wizard. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /forwarder <type> /tunnel Port Forwarder Tunnel Configuration on page 346.
app
Lets you specify the application to be started when the user clicks the port forwarder link. The **app** command corresponds to the application path step in the Quick Setup wizard.
appargs
Lets you specify the argument to the application. The **appargs** command corresponds to the application arguments step in the Quick Setup wizard.
splash
Lets you specify the text to appear in the Java applet window if you want custom user instructions to be displayed. The **splash** command corresponds to the application arguments step in the Quick Setup wizard.
phost

Command Syntax and Usage
Lets you specify the IP address or domain name of an intermediate intranet HTTP Proxy server, if users are working from a location requiring traffic to pass through such a proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. The **phost** command corresponds to the HTTP proxy host step in the Quick Setup wizard.
pport
Lets you specify the port number of an intermediate intranet HTTP Proxy server. The **pport** command corresponds to the HTTP proxy port step in the Quick Setup wizard.
puser
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **puser** command corresponds to the HTTP proxy user name step in the Quick Setup wizard.
ppass
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **ppass** command corresponds to the HTTP proxy password step in the Quick Setup wizard.

/cfg/vpn <id> /linkset <id> /link <id> /forwarder <type> /tunnel Port Forwarder Tunnel Configuration

```
[Tunnel 1 Menu] tmode- Set traffic mode
lhost- Set local host
lport- Set local port
rhost- Set remote host
rport- Set remote port
hmap - Set host mapping
del  - Remove tunnel
```

The Tunnel menu includes commands to edit the tunnel properties of an existing Port forwarder link.

Table 182: Tunnel Menu (/cfg/vpn/linkset/link/forwarder/tunnel)

Command Syntax and Usage
tmode <*TCP/UDP*>

Command Syntax and Usage
Lets you specify which network protocol (UDP or TCP) should be used for the selected tunnel.
lhost
Lets you edit the local host IP address for the selected tunnel. The local host IP address is the IP address associated with the client computer. The local host IP address can for example be **127.0.0.1** or any other IP address in the 127.x.y.z range.
lport
Lets you edit the local port number for the selected tunnel. Ports just preceding 5000 are usually free to use.
rhost
Lets you edit the remote host IP address for the selected tunnel. The remote host IP address is the IP address associated with the application server.
rport
Lets you edit the remote host port number for the selected tunnel. The remote host port number is the application-specific port number of the application server, e.g. **80** for HTTP traffic.
hmap
Lets you edit the alias that identifies the local host. Aliases can be specified to provide easy access when no executable has been specified, that is, the user should start the application manually. The user starts by clicking the port forwarder link to set up the tunnel. The next step is to start the client application and connect to the application server. Example: Suppose the application is Telnet, the local host IP address is 127.0.0.1 and the local port number is 5025. The remote host is telnet.example.com. By entering a suitable host alias (for example telnet.example.com or simply telnet) with the hmap command, the user can connect to telnet.example.com 5025 (or telnet 5025) instead of the less intuitive 127.0.0.1 5025. The host alias should be mentioned in the Java applet text (specified with the **splash** command). It also requires the user to have administrator privileges on the client 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.

/cfg/vpn <id> /linkset <id> /link <id> /forwarder <mail> Mail Port Forwarder Link Configuration

```
[Port forwarder settings Menu]
quick      - Quick port forwarder wizard
tunnel     - Tunnel menu
app  - Set application path
appargs    - Set application arguments
splash     - Set splash text in Applet window
phost- Set proxy host
pport- Set proxy port
puser- Set proxy username
ppass- Set proxy password
```

The Port Forwarder Settings menu for a port forwarder of the mail type includes the same commands as for the other port forwarder types. The Quick Setup wizard (invoked with the **quick** command) prompts you for information specific for a mail server connection.

Table 183: Port Forwarder Settings Menu (/cfg/vpn/linkset/link/forwarder)

Command Syntax and Usage
quick (mail) *<SMTP local host IP> <SMTP local port> <SMTP remote host> <SMTP remote port> <SMTP host mapping> <IMAP4 local host IP> <IMAP4 local port> <IMAP4 remote host> <IMAP4 remote port> <IMAP4 host mapping> <POP3 local host IP> <POP3 local port> <POP3 remote host> <POP3 remote port> <POP3 host mapping> <application path> <application arguments> <text to be displayed in applet window> <HTTP proxy host and port> <HTTP proxy host user name and password>* Lets you run a wizard to create a mail port forwarder link. Configuration is similar to the custom port forwarder. The only difference is that the wizard suggests values (for SMTP, IMAP4 and POP3) that are appropriate to a mail connection. • Local host IP address. Sets the IP address associated with the client computer, e.g. **127.0.0.1** or any other IP address in the 127.x.y.z range. • Local port. Arbitrary local port number. The wizard suggests the applications-specific port so that you do not have to change reconfigure the mail client. • Remote host. Sets the IP address or host name of the remote mail server. • Remote port. Sets the application-specific port number of the service (SMTP, IMAP4 and POP3 respectively). • Host mapping. See the custom port forwarder for a detailed description. • Application path (optional). Defines the mail client to be started when the user clicks the link. The wizard suggests **outlook.exe**, that is, Microsoft Outlook. Note that Microsoft Outlook can only be used as mail client if set to Internet mode. If the remote users' Microsoft Outlook clients are set to Corporate mode, use the

Command Syntax and Usage
Outlook port forwarder instead. To start Outlook Express as the mail client, enter **msimn.exe** as executable. • Application arguments (optional). For more information about available arguments for the selected mail client, see the corresponding documentation. • Text. Replaces the standard text in the Java applet window, that is, more user-friendly instructions can be supplied. Having entered the text, press ENTER and type three periods (...). Finally press ENTER once again. To keep the standard text (information about host file mappings and opened sockets), type three periods and press ENTER. • HTTP proxy host/port. If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password.
tunnel
Displays the Tunnel menu where you can edit the tunnel specifics of the current port forwarder link, that is, traffic mode, local host/port, remote host/port and host mapping. The commands on the Tunnel menu correspond to the first five steps in the Quick Setup wizard. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /forwarder <type> /tunnel Port Forwarder Tunnel Configuration on page 346.
app
Lets you specify the application to be started when the user clicks the port forwarder link. The **app** command corresponds to the application path step in the Quick Setup wizard.
appargs
Lets you specify the argument to the application. The **appargs** command corresponds to the application arguments step in the Quick Setup wizard.
splash
Lets you specify the text to appear in the Java applet window if you want custom user instructions to be displayed. The **splash** command corresponds to the application arguments step in the Quick Setup wizard.
phost

Command Syntax and Usage
Lets you specify the IP address or domain name of an intermediate intranet HTTP Proxy server, if users are working from a location requiring traffic to pass through such a proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. The **phost** command corresponds to the HTTP proxy host step in the Quick Setup wizard.
pport
Lets you specify the port number of an intermediate intranet HTTP Proxy server. The **pport** command corresponds to the HTTP proxy port step in the Quick Setup wizard.
puser
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **puser** command corresponds to the HTTP proxy user name step in the Quick Setup wizard.
ppass
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **ppass** command corresponds to the HTTP proxy password step in the Quick Setup wizard.

/cfg/vpn <id> /linkset <id> /link <id> /forwarder <telnet> Telnet Port Forwarder Link Configuration

```
[Port forwarder settings Menu]
quick      - Quick port forwarder wizard
tunnel     - Tunnel menu
app  - Set application path
appargs    - Set application arguments
splash     - Set splash text in Applet window
phost- Set proxy host
pport- Set proxy port
puser- Set proxy username
ppass- Set proxy password
```

The Port Forwarder Settings menu for a port forwarder of the telnet type includes the same commands as for the other port forwarder types. The Quick Setup wizard (invoked with the **quick** command) prompts you for information specific for a Telnet connection.

Table 184: Port Forwarder Settings Menu (/cfg/vpn/linkset/link/forwarder)

Command Syntax and Usage
quick (telnet) *<local host IP> <local port> <remote TELNET host> <remote TELNET port> <host mapping> <application path> <application arguments> <text to be displayed in applet window> <HTTP proxy host and port> <HTTP proxy host user name and password>* Lets you run a wizard to create a Telnet port forwarder link. Configuration is done almost exactly as for the custom port forwarder. The only difference is that the wizard suggests values that are appropriate for a Telnet connection. • Local host IP address. Sets the IP address associated with the client computer, e.g. 127.0.0.1 or any other IP address in the 127.x.y.z range. • Source port. Arbitrary local port number. Ports just preceding 5000 are usually free to use. • Remote Telnet host. Sets the IP address or host name of the remote Telnet server, e.g. 192.168.128.211. • Remote Telnet port. Sets the application-specific port number for a Telnet connection, that is, 23. • Host mapping (see the **custom** option for a detailed description). • Application path (optional). Defines the application to be started when the user clicks the link. The wizard suggests **cmd.exe** as executable which means that the Telnet session will be run in the Command window. • Application arguments (optional). Defines the command-line argument to be used by the application, in this case the source IP address and source port number (e.g. 127.0.0.1 5005). • Text. Replaces the standard text in the Java applet window, that is, more user-friendly instructions can be supplied. Having entered the text, press ENTER and type three periods (...). Finally press ENTER once again. To keep the standard text (information about host file mappings and opened sockets), type three periods and press ENTER. • HTTP proxy host/port. If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password.
tunnel Displays the Tunnel menu where you can edit the tunnel specifics of the current port forwarder link, that is, traffic mode, local host/port, remote host/port and host mapping. The commands on the Tunnel menu correspond to the first five steps in the Quick Setup wizard.

Command Syntax and Usage
To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /forwarder <type> / tunnel Port Forwarder Tunnel Configuration on page 346.
app
Lets you specify the application to be started when the user clicks the port forwarder link. The **app** command corresponds to the application path step in the Quick Setup wizard.
appargs
Lets you specify the argument to the application. The **appargs** command corresponds to the application arguments step in the Quick Setup wizard.
splash
Lets you specify the text to appear in the Java applet window if you want custom user instructions to be displayed. The **splash** command corresponds to the application arguments step in the Quick Setup wizard.
phost
Lets you specify the IP address or domain name of an intermediate intranet HTTP Proxy server, if users are working from a location requiring traffic to pass through such a proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. The **phost** command corresponds to the HTTP proxy host step in the Quick Setup wizard.
pport
Lets you specify the port number of an intermediate intranet HTTP Proxy server. The **pport** command corresponds to the HTTP proxy port step in the Quick Setup wizard.
puser
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **puser** command corresponds to the HTTP proxy user name step in the Quick Setup wizard.
ppass
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **ppass** command corresponds to the HTTP proxy password step in the Quick Setup wizard.

/cfg/vpn <id> /linkset <id> /link <id> /forwarder <netdrive> Netdrive Port Forwarder Link Configuration

```
[Port forwarder settings Menu]
quick      - Quick port forwarder wizard
tunnel     - Tunnel menu
app  - Set application path
appargs    - Set application arguments
splash     - Set splash text in Applet window
phost- Set proxy host
pport- Set proxy port
puser- Set proxy username
ppass- Set proxy password
```

The Port Forwarder Settings menu for a port forwarder of the netdrive type includes the same commands as for the other port forwarder types. The Quick Setup wizard (invoked with the **quick** command) prompts you for information specific for mapping a network drive.

Table 185: Port Forwarder Settings Menu (/cfg/vpn/linkset/link/forwarder)

Command Syntax and Usage
quick (netdrive) *<local host IP> <local port> <remote network drive mapping host> <remote network drive mapping port> <application path> <application arguments> <text to be displayed in applet window> <HTTP proxy host and port> <HTTP proxy host user name and password>* Lets you run a wizard to create a port forwarder link for mapping a shared network drive on a remote host to the users file system. The network drive will be displayed for example in Windows Explorer and in the My Computer view. Configuration is done almost exactly as for the custom port forwarder. The wizard suggests the values that are appropriate for mapping a network drive using Windows' built-in net service commands. **Note:** Network drive mapping is not supported on Windows 98 and XP clients. • Local host IP address. Sets the IP address associated with the client computer, e.g. 127.0.0.2 or any other IP address in the 127.x.y.z range. • Local port. Arbitrary local port number. The wizard suggests 139, which is the application-specific port number for SMB (Windows file share) servers. • Remote host. Sets the IP address or host name of the remote server. • Remote port. Sets the application-specific port number of the service, that is, 139. • Application path (optional). Defines the application to be started when the user clicks the link. The wizard suggests **net.exe**.

Command Syntax and Usage
• Application arguments (optional). For information about available arguments, go to the Windows Help system and search for **net use**. The argument suggested by the wizard will map the next free drive label (for example L:) to 127.0.0.2. The user name and password used for Portal login are used to authenticate the user to the remote file share. • Text. Replaces the standard text in the Java applet window, that is, more user-friendly instructions can be supplied. Having entered the text, press ENTER and type three periods (...). Finally press ENTER once again. To keep the standard text (information about host file mappings and opened sockets), type three periods and press ENTER. • HTTP proxy host/port. If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password.
tunnel
Displays the Tunnel menu where you can edit the tunnel specifics of the current port forwarder link, that is, traffic mode, local host/port, remote host/port and host mapping. The commands on the Tunnel menu correspond to the first five steps in the Quick Setup wizard. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /forwarder <type> /tunnel Port Forwarder Tunnel Configuration on page 346.
app
Lets you specify the application to be started when the user clicks the port forwarder link. The **app** command corresponds to the application path step in the Quick Setup wizard.
appargs
Lets you specify the argument to the application. The **appargs** command corresponds to the application arguments step in the Quick Setup wizard.
splash
Lets you specify the text to appear in the Java applet window if you want custom user instructions to be displayed. The **splash** command corresponds to the application arguments step in the Quick Setup wizard.
phost

Command Syntax and Usage
Lets you specify the IP address or domain name of an intermediate intranet HTTP Proxy server, if users are working from a location requiring traffic to pass through such a proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. The **phost** command corresponds to the HTTP proxy host step in the Quick Setup wizard.
pport
Lets you specify the port number of an intermediate intranet HTTP Proxy server. The **pport** command corresponds to the HTTP proxy port step in the Quick Setup wizard.
puser
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **puser** command corresponds to the HTTP proxy user name step in the Quick Setup wizard.
ppass
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **ppass** command corresponds to the HTTP proxy password step in the Quick Setup wizard.

/cfg/vpn <id> /linkset <id> /link <id> /forwarder <wts> WTS Port Forwarder Link Configuration

```
[Port forwarder settings Menu]
quick      - Quick port forwarder wizard
tunnel     - Tunnel menu
app  - Set application path
appargs    - Set application arguments
splash     - Set splash text in Applet window
phost- Set proxy host
pport- Set proxy port
puser- Set proxy username
ppass- Set proxy password
```

The Port Forwarder Settings menu for a port forwarder of the wts type includes the same commands as for the other port forwarder types. The Quick Setup wizard (invoked with the **quick** command) prompts you for information specific for setting up a connection to a Windows Terminal Server.

Table 186: Port Forwarder Settings Menu (/cfg/vpn/linkset/link/forwarder)

Command Syntax and Usage
quick (wts) *<local host IP> <local port> <remote desktop connection host> <remote desktop connection port> <host alias> <application path> <application arguments> <text to be displayed in applet window> <HTTP proxy host and port> <HTTP proxy host user name and password>* Lets you run a wizard to create a port forwarder link to a Windows Terminal Server. Configuration is done almost exactly as for the custom port forwarder. The wizard simply suggests values that are appropriate for this port forwarder type. • Local host IP address. Sets the IP address associated with the client computer, e.g. 127.0.0.2 or any other IP address in the 127.x.y.z range. • Local port. Arbitrary local port number. The wizard suggests 3390, which is the application-specific port number for Windows Terminal Server. • Remote host. Sets the IP address or host name of the remote desktop connection server. • Remote port. Sets the application-specific port number of the service, that is, 3389. • Host mapping (see the **custom** option for a detailed description). • Application path (optional). Defines the application to be started when the user clicks the link. The wizard suggests **mstsc.exe**. • Application arguments (optional). For more information about available arguments for Windows Terminal Server, see the corresponding documentation. The argument suggested in the wizard means that the terminal server client should connect to a server listening on IP address 127.0.0.2, port 3390, using a window size of 800 x 600. • Text. Replaces the standard text in the Java applet window, that is, more user-friendly instructions can be supplied. Having entered the text, press ENTER and type three periods (...). Finally press ENTER once again. To keep the standard text (information about host file mappings and opened sockets), type three periods and press ENTER. • HTTP proxy host/port. If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password.
tunnel Displays the Tunnel menu where you can edit the tunnel specifics of the current port forwarder link, that is, traffic mode, local host/port, remote host/port and host mapping.

Command Syntax and Usage
The commands on the Tunnel menu correspond to the first five steps in the Quick Setup wizard. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /forwarder <type> /tunnel Port Forwarder Tunnel Configuration on page 346.
app
Lets you specify the application to be started when the user clicks the port forwarder link. The **app** command corresponds to the application path step in the Quick Setup wizard.
appargs
Lets you specify the argument to the application. The **appargs** command corresponds to the application arguments step in the Quick Setup wizard.
splash
Lets you specify the text to appear in the Java applet window if you want custom user instructions to be displayed. The **splash** command corresponds to the application arguments step in the Quick Setup wizard.
phost
Lets you specify the IP address or domain name of an intermediate intranet HTTP Proxy server, if users are working from a location requiring traffic to pass through such a proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. The **phost** command corresponds to the HTTP proxy host step in the Quick Setup wizard.
pport
Lets you specify the port number of an intermediate intranet HTTP Proxy server. The **pport** command corresponds to the HTTP proxy port step in the Quick Setup wizard.
puser
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **puser** command corresponds to the HTTP proxy user name step in the Quick Setup wizard.
ppass
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **ppass** command corresponds to the HTTP proxy password step in the Quick Setup wizard.

/cfg/vpn <id> /linkset <id> /link <id> /forwarder <outlook> Outlook Port Forwarder Link Configuration

```
[Port forwarder settings Menu]

quick          - Quick port forwarder wizard

tunnel         - Tunnel menu

app            - Set application path

appargs        - Set application arguments

splash         - Set splash text in Applet window

phost          - Set proxy host

pport          - Set proxy port

puser          - Set proxy username

ppass          - Set proxy password
```

The Port Forwarder Settings menu for a port forwarder of the outlook type includes the same commands as for the other port forwarder types. The Quick Setup wizard (invoked with the **quick** command) prompts you for information specific for setting up a connection to a Microsoft Exchange server.

Table 187: Port Forwarder Settings Menu (/cfg/vpn/linkset/link/forwarder)

Command Syntax and Usage
quick (outlook) *<local host IP> <Exchange server FQDN> <another port forwarder> <application path> <application arguments> <text shown in applet window> <HTTP proxy host and port> <HTTP proxy host user name and password>* Creates a Port forwarder link for starting Microsoft Outlook towards a Microsoft Exchange server on the intranet. Services provided by the Exchange server (mail, calendar, address book and so on.) may be distributed between different Exchange servers. If this is the case, you have the option to create several Outlook port forwarders where the relevant Exchange servers can be specified.

Command Syntax and Usage

Important:

The following prerequisites must be fulfilled for the Outlook Port forwarder to work:

- The Exchange servers' domain name suffixes, e.g. example.com if the FQDN is exchange.example.com, must be configured using the **/cfg/ssl/server #/ dns/search** command.
- 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 user's client machine must be of the **Hybrid** or **Unknown node** type. The node type can be checked by entering **ipconfig /all** at the DOS prompt. To change the node type to Hybrid (if needed), go to the registry editor folder HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters. If not already present, add a new DWORD Value called NodeType. Double-click NodeType and enter 8 in the Value Data field. Click OK and restart the computer.
- The Outlook Port forwarder link is meant to be used by clients connecting to the VPN Gateway from outside the intranet. If the client has direct connectivity to the intranet, the Port forwarder will fail. If the client has access to intranet DNS servers, communication will fail as well.
- To test DNS resolution, the VPN Gateway should be able to ping the Exchange server from the CLI, using the fully qualified domain name (FQDN).
- 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.
- The users Outlook account must be hosted on the Exchange server(s) specified in the Port forwarder.
- If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value, using the **/cfg/vpn <id>/server/tcp/ckeep** command.
- If a firewall exists between the VPN Gateway and the Exchange server, the firewall settings must allow traffic to the required Exchange server ports. Note that these may vary with your environment. More information can be found on http://support.microsoft.com, for example Knowledge Base Articles 280132, 270836, 155831, 176466, 148732, 155831, 298369, 194952, 256976, 302914, 180795 and 176466.
- When a user clicks an embedded link in an e-mail message, the web site associated with the link must be displayed in a new instance of Internet Explorer. In Internet Explorer, go to the Tools menu and select Internet

Command Syntax and Usage
Options. Under the Advanced tab, go to Browsing and deselect the "Reuse windows for launching shortcuts" option. Command syntax and usage: • Local host IP address. Sets the IP address associated with the client computer, e.g. 127.0.0.1or any other IP address in the 127.x.y.z range. 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. • Exchange server. Sets the fully qualified domain name (FQDN) of the Exchange server, e.g. exchange.example.com. • Yet another port forwarder. If mailboxes, calendars, address books and so on. are delegated to several Exchange servers, you have the option to create additional Port forwarders where the relevant Exchange server FQDNs can be specified. • Application path. Defines the application to be started when the user clicks the link. The wizard suggests **`outlook.exe`**. • Argument to Outlook client. Example: **`/Profile myprofile`**. For a reference to available Outlook executable arguments, see Microsoft Knowledge Base Article no 296192 available on http://support.microsoft.com/?kbid=296192. • Text. Replaces the standard text in the Java applet window, for example if more user-friendly instructions should be supplied. Having entered the text, press ENTER and type three periods (...). Finally press ENTER once again. To keep the standard text (information about host file mappings and opened sockets), type three periods and press ENTER. • HTTP proxy host/port. If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. For a configuration example, see the "Group Links" chapter in the *Application Guide for VPN*.
`tunnel`
Displays the Tunnel menu where you can edit the tunnel specifics of the current port forwarder link, that is, traffic mode, local host/port, remote host/port and host mapping. The commands on the Tunnel menu correspond to the first five steps in the Quick Setup wizard. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /forwarder <type> /tunnel Port Forwarder Tunnel Configuration on page 346.

Command Syntax and Usage
app
Lets you specify the application to be started when the user clicks the port forwarder link. The **app** command corresponds to the application path step in the Quick Setup wizard.
appargs
Lets you specify the argument to the application. The **appargs** command corresponds to the application arguments step in the Quick Setup wizard.
splash
Lets you specify the text to appear in the Java applet window if you want custom user instructions to be displayed. The **splash** command corresponds to the application arguments step in the Quick Setup wizard.
phost
Lets you specify the IP address or domain name of an intermediate intranet HTTP Proxy server, if users are working from a location requiring traffic to pass through such a proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. The **phost** command corresponds to the HTTP proxy host step in the Quick Setup wizard.
pport
Lets you specify the port number of an intermediate intranet HTTP Proxy server. The **pport** command corresponds to the HTTP proxy port step in the Quick Setup wizard.
puser
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **puser** command corresponds to the HTTP proxy user name step in the Quick Setup wizard.
ppass
If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password. The **ppass** command corresponds to the HTTP proxy password step in the Quick Setup wizard.

/cfg/vpn <id> /linkset <id> /link <id> /wts Window terminal server configuration

```
wts menu Menu

quick           - Quick wts forwarder wizard
tunnel          - Tunnel menu
domain          - Set domain name
app             - Set application path
workingdir      - Set working directory
screensize      - Set screen size
colordepth      - Set color depth
mapdrive        - Set map local drives
clipboard       - Set enable clipboard redirection.
mapprinter      - Set connect local printers client
enablesso       - Set enable single sign on
winostype       - Set Windows OS type
javaclient      - Set enable Java RDP as default client
hidepf          - Set hide port forwarder window
splash          - Set splash text in Applet window
phost           - Set proxy host
pport           - Set proxy port
```

```
puser             - Set proxy username

ppass             - Set proxy password
```

An ActiveX and Java version of the WTS client enables the installation of WTS client on demand. WTS client can be run on the following servers:

- Windows 2000 server
- Windows 2003 server – Standard Edition
- Windows 2003 server – Enterprise Edition

The wts menu, enables the configuration of following parameters:

- Screen resolution
- Color depth
- Enable local drive mapping
- Enable local printer mapping
- Application to start after logon
- Enable single sign-on
- Enable Java version as the default client

Table 188: WTS menu (/cfg/vpn <id>/linkset <>id/link/wts)

Command Syntax and Usage
quick
Allows you to run through the quick wizard to setup a WTS link. It suggests same defaults for most of the items.
tunnel
This is same as the tunnel setup for a port forwarder.
domain
This is the domain name.
app
This is the application path to start automatically after connecting. This refers to an application on the WTS server.
workingdir
This is the path to be used as the current working directory on the WTS server. Some applications may need the workingdir to be set for proper functioning.
workingdir

Command Syntax and Usage
Screen size for the WTS session. Possible values are ‘Full Screen’, ‘800x600’, ‘1074x768’ and ‘1280x1024’. Default is ‘800x600’
screensize
Screen size for the WTS session. Possible values are ‘Full Screen’, ‘800x600’, ‘1074x768’ and ‘1280x1024’. 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’.
mapdrive
Select whether local drives are mapped in the WTS session as network drives. Possible values are ‘on’ and ‘off’. Default is ‘off’.
mapprinter
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.
clipboard
This commands lets you enable or disable the clipboard redirection.
enablesso
Select whether to automatically sign in the user into the WTS session using the credentials used to login to the portal.
winostype
Select the JavaRDP applet for client OS. Possible values are ‘Windows’ and ‘Windows2008’. Default is ‘Windows’.
javaclient
By default, the portal tries to use the ActiveX client and falls back to Java if that fails. This menu items allows the administrator to make Java the default client. Possible values are ‘on’ and ‘off’, Default is ‘off’.
hidepf
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.
splash
Setup custom text to display in the port forwarder window. Meaningful only when ‘hidepf’ is set to ‘off’.
phost

Command Syntax and Usage
If the traffic is needed to go through an http proxy between the client PC and AVG, please enter the IP address or domain name of the proxy server here.
pport
Relevant only when phost is set. Use this to set the port on the http proxy to connect to. Default value is 'none'. If phost is set. then pport should be set to some number between 1 and 65535.
puser
Relevant only if host is set. If the proxy server requires authentication, enter the user name here. If no authentication is required, leave this empty. Maximum allowed length is 128.
ppass
Relevant only when phost and puser are set. If the http proxy requires authentication, enter the password here. Maximum allowed length is 128.

/cfg/vpn <id> /linkset <id> /link <id> /citrix Citrix configuration

```
[Citrix Menu]

quick           - Quick citrix setup wizard

mode            - Set Select Citrix mode

address         - Set Address

serverport      - Set ServerPort

icabrowser      - Set icabrowser list

initpgm         - Set Initial Program

screensize      - Set screen size

colordepth      - Set color depth

mapdrive        - Set map local drives
```

```
mapprinter        - Set connect local printers

settingdlg        - Set show settings button

enabletzon        - Set enable adding domain to trusted zone

javaclient        - Set enable Java as default citrix client

enablesso         - Set enable single sign on
```

An ActiveX and Java version of the Citrix client enables the installation of citrix client on demand. Citrix client can be run on the Citrix Presentation server 4.x Standard Editionservers.

The Citrix menu, enables the configuration of following parameters:

- Screen resolution
- Color depth
- Enable local drive mapping
- Enable local printer mapping
- Application to start after logon
- Enable single sign-on
- Enable Java version as the default client

Table 189: Citrix menu (/cfg/vpn/linkset/link/Citrix)

Command Syntax Usage
quick Runs you through the quick setup wizard to setup a Citrix link. It suggests same defaults for most of the items.
mode When mode is desktop, address should be displayed and also initpgm should be displayed". Suppose if the mode is application address should not be displayed instead 3 icabrowser should be displayed and initpgm should be hided from menu.
address Specify the DNS name or IP address of the shared Citrix desktop to connect to. You cannot configure both ‘address’ and ‘app’ (you either connect to an application or a desktop, not both). You also don’t have to configure any ‘icabrowser’ when address is specified. The ‘icabrowser’ setting is ignored when ‘address’ is set.

Command Syntax Usage
serverport
If the Citrix server uses a non-standard port, please specify it here. Default value is 1494. Valid range is 1 through 65535.
icabrowser
‘ICA Browsers’ are part of the Citrix setup. They provide redundancy and load balancing for the actual Citrix server behind them. For sharing (publishing) applications, setting up ICA browsers is mandatory. Use the ‘icabrowser’ menu to setup the list of ICA browsers. A maximum of 3 ICA browsers are allowed. The DNS name or IP address can be used to specify the ICA browser. The application name specified using ‘app’ should be published on at least one of the ICA browsers specified.
initpgm
Specify initial program to run when connecting to a Citrix desktop. By default this is empty which means no applications will startup. You may specify a path to an application within the Citrix desktop to have it start up automatically on connection. This setting is applicable only when ‘address’ is set and ignored when ‘app’ is set.
workingdir
Path to be used as the current working directory inside the Citrix session. Some applications may need the workingdir to be set for proper functioning.
screensize
Screen size for the Citrix session. Possible values are ‘Full Screen’, ‘800x600’, ‘1074x768’ and ‘1280x1024’. Default is ‘800x600’.
colordepth
Color depth for the Citrix session. Possible values are ‘8 bit’, ‘15 bit’, ‘16 bit’, ‘24 bit’ and ‘32 bit (True Color)’. Default value is ‘16 bit’.
mapdrive
Select whether local drives are mapped within the Citrix session as network drives. Possible values are ‘on’ and ‘off’, Default is ‘off’. Enable ‘settingdlg’ to let the user enable this feature manually when using the Java client.
mapprinter
Select whether local printers are available in the WTS session. Possible values are ‘on’ and ‘off’, Default is ‘off’. Enable ‘settingdlg’ to let the user enable this feature manually when using the Java client.
settingdlg
This setting is applicable only to the Java client. It can be used to enable the end user to access the ‘Settings’ dialog of the client and setup drive mapping and printer mapping manually. The Java client does not support setting this up automatically without end user intervention.

Command Syntax Usage
enabletzon
This setting is applicable only to the ActiveX client. The ActiveX client requires AVG to be added to the 'Trusted zone' of MSIE browser to function properly. If this setting is enabled, AVG will try to add itself to the trusted zone if needed. However this will work only if the end user has administrative rights on the PC. If Citrix fails to launch due to AVG not being in the trusted zone, an error message will be displayed to the user explaining how to add AVG to the trusted zone manually.
enablesso
Select whether to automatically sign in the user into the Citrix session using the credentials used to login to the portal. SSO will work both for published applications ('app') as well as desktops.
javaclient
By default, the portal tries to use the Java client and falls back to ActiveX if that fails. This menu items allows the administrator to make Java the default client. this makes Java Possible values are 'on' and 'off', Default is 'on'. The reason for making Java the default is that the ActiveX control requires AVG to be added to the 'Trusted zone' of the browser to work.

/cfg/vpn <id> /linkset <id> /link <id> /netdirect Net Direct Link Configuration

```
[Net Direct menu]
quick- Quick Net Direct link wizard
```

The Net Direct menu lets you create a link on the Portal that downloads and launches the Net Direct VPN client. The Net Direct client runs in the background on the remote user's PC. When active, any native client TCP- or UDP-based application can be run towards an intranet application server. No further Portal interaction is required to access intranet resources. The remote user's access rights determine whether or not the requested server is accessible.

Apart from creating a Net Direct link, you should enable Net Direct client access, using the **/cfg/vpn <id>/sslclient/netdirect/on** command. In addition, you should configure at least one IP pool with the desired method for IP address assignment (see the **/cfg/vpn <id> /ippool** command on /cfg/vpn <id> /ippool <id> IP Pool Configuration on page 307). Finally, one of the configured IP pools should be selected as the default IP pool.

If Net Direct is not enabled when you attempt to configure the Net Direct link, you will be prompted for the required information in the wizard when you configure the link.

For detailed step-by-step instructions on how to configure the VPN Gateway for use with the Net Direct client, see the "Net Direct" chapter in the *Application Guide for VPN*.

Table 190: Net Direct Menu Options (/cfg/vpn/linkset/link/netdirect)

Command Syntax and Usage
quick (netdirect) Lets you run a wizard for creating a Net Direct link on the Portal's Home tab. If Net Direct is enabled and an IP pool has already been configured, the Net Direct link is automatically created. If Net Direct is not enabled or if no IP pool exists, a wizard will prompt you for the required information. • Enable Net Direct client (yes/no): Equivalent to enabling Net Direct using the **/cfg/vpn <id>/sslclient/netdirect/on** command (see /cfg/vpn <id>/sslclient Net Direct and SSL VPN Client Configuration on page 377). • Lower/upper IP address in pool range: Lets you set the IP address range for a local IP address pool. Also see the **/cfg/vpn <id>/ippool** command on /cfg/vpn <id> /ippool <id> IP Pool Configuration on page 307. • Primary DNS server: IP address of primary DNS server (optional). If no IP address is specified here, the global DNS server settings will be used (see **/cfg/sys/dns/servers** on /cfg/vpn <id> /adv/dns/servers DNS Servers Configuration on page 393).

/cfg/vpn <id> /linkset <id> /link <id> /terminal Terminal Link Configuration

```
[Terminal Settings Menu]
quick- Quick terminal link wizard
```

The Terminal Settings menu lets you edit an existing terminal server link. Terminal server links are displayed on the Portal's Home tab. 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. For the user to be able to type anything in the terminal window, it must be activated by clicking on it.

Table 191: Terminal Settings Menu Options (/cfg/vpn/linkset/link/terminal)

Command Syntax and Usage
quick (terminal) *<remote host> <port number [23|22]> <protocol [ssh|sshv2|telnet]> <keymap URL> <HTTP proxy host and port (optional)> <HTTP proxy user name and password>*

Command Syntax and Usage
Lets you run a wizard for creating a direct link to a terminal server, using Telnet or SSH. The wizard will ask you for the following information: • Remote host. Sets the IP address or host name of the remote terminal server. • Remote port. Sets the application-specific port number of the service, that is, 23 (Telnet) or 22 (SSH). • Protocol. Sets the desired protocol, that is, SSH version 1, SSH version 2 or Telnet. • Keymap URL (optional). 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 is 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 can be found in Appendix F, "Definition of Key Codes", in the *User's Guide*. • HTTP Proxy host/port (optional). If users are working from a location requiring traffic to pass through an intermediate intranet HTTP Proxy server, enter the IP address (or domain name) and port of that proxy server. Skipping the prompt means that all applet traffic is tunneled straight to the VPN Gateway. • HTTP Proxy user name/password. If a HTTP Proxy host/port is specified and the HTTP Proxy host requires authentication, you have the option to enter a user name and password.

/cfg/vpn <id> /linkset <id> /link <id> /external External Link Configuration

```
[External Settings Menu]
quick- Quick external link wizard
```

The External Settings menu lets you edit or create a link of the external type. Both the external and internal link types are designed to direct the remote user to a web page. The difference between an external and an internal link is that the external link is not secured by the VPN Gateway.

The external link directs the HTTP or HTTPS request straight to the specified resource, that is, without adding the AVG rewrite prefix to the URL (compare to the internal link described on /cfg/vpn <id> /linkset <id> /link <id> /internal Internal Link Configuration on page 371).

Table 192: External Settings Menu Options (/cfg/vpn/linkset/link/external)

Command Syntax and Usage
quick (external) *<method [http|https]> <web server by IP address or host name> <path>* Lets you run a wizard for creating a link to a web page or web resource, accessed by using HTTP or HTTPS. • Method. HTTP or HTTPS. • Host. Web server by IP address or host name, e.g. www.example.com. • Path. A path must always be specified, where a single backslash (/) indicates the web server's document root.

/cfg/vpn <id> /linkset <id> /link <id> /internal Internal Link Configuration

```
[Internal Settings Menu]
quick- Quick internal link wizard
```

The Internal Settings menu lets you edit or create a link of the internal type. Both the external and internal link types are designed to direct the remote user to a web page. The difference between an external and an internal link is that the internal link is secured by the VPN Gateway, that is, the internal link directs the HTTP/HTTPS request to the VPN Gateway, where the AVG rewrite prefix (boldface) is added to the link.

Example: https://portal.example.com/http/inside.example.com/

This way, you are guaranteed that the request is sent through a secure connection through SSL.

Table 193: Internal Settings Menu Options (/cfg/vpn/linkset/link/internal)

Command Syntax and Usage
quick (internal) *<method [http|https]> <web server by IP address or host name> <path>* Lets you run a wizard for creating a link to a web page or web resource, accessed by using HTTP or HTTPS. • Method. HTTP or HTTPS. • Host. Web server by IP address or host name, e.g. inside.example.com. • Path. A path must always be specified, where a single backslash (/) indicates the web server's document root.

Command Syntax and Usage
To create a link to the currently logged in SSL VPN user's home page on the intranet, you can use the following macro when prompted for the path: • */<var:user>:* This macro automatically replaces *<var:user>* with the currently logged in SSL VPN user's user name, and thereby provides access to that user's home page. **Note:** Depending on how the intranet web server is configured, you may need to insert an additional character to specify the correct path. Example: */~<var:user>*.

/cfg/vpn <id> /linkset <id> /link <id> /iauto Iauto Link Configuration

```
[Iauto Settings Menu]
quick- Quick internal auto login link wizard
type - Set authentication type
method     - Set HTTP or HTTPS
host - Set internal host
path - Set path on internal server
proxy- Use this as a proxy link
mapping    - Post/Get data
cookies    - Post/Get cookies
mode - Set Basic auth mode
```

The Iauto Settings menu lets you edit or create a link of the iauto type. The iauto link provides automatic login access to a password-protected web page through a secure SSL connection. This feature is useful when a web server requires user authentication, such as a web server providing Outlook Web Access.

The `iauto` link directs the HTTP request to the VPN Gateway where the rewrite prefix (boldface) is added to the link. See example below:

`https://portal.example.com/https/inside.example.com/login/login.asp`

The VPN Gateway manages authentication to the backend server. This ensures that user name and password will not be visible in the client browser.

The **`iauto`** link supports form-based authentication as well as HTTP-based authentication, such as NTLM or basic (www-authenticate). When you have entered the URL following the **`iauto`** command, the VPN Gateway automatically retrieves the URL to analyze which type of authentication method it uses. The result is displayed in the CLI:

- If the specified URL uses HTTP-based authentication, a message will confirm this and the link is complete. The remote user will automatically be logged on to this web page if

the credentials are the same as those provided on the Portal. If not, a form will be displayed for the user to provide the required credentials.

- If the specified URL uses form-based authentication, the input fields found on the web page will be displayed in the CLI for you to specify which values to insert. The <*var:user*> and <*var:password*> macros expand to the logged in Portal user's credentials. The <*var:domain*> macro expands to the domain name specified for the current authentication method, using the **/cfg/vpn <id>/aaa/auth <id>/domain** command (see /cfg/vpn <id> /aaa/auth <id> Authentication Method Configuration on page 165).

Table 194: Iauto Settings Menu Options (/cfg/vpn/linkset/link/iauto)

Command Syntax and Usage
quick (iauto) <*URL*> Lets you run a wizard for creating an automatic login link to a password-protected web page. • Login URL. Enter the URL to the password-protected web page, e.g. https://inside.example.com/login/login.asp. • Values for input fields found on form. Specify which values to insert in the fields when the remote user clicks the iauto link. The <*var:user*> and <*var:password*> macros expand to the logged in Portal user's credentials. The <*var:domain*> macro expands to the domain name specified for the current authentication method, using the **/cfg/vpn <id>/aaa/auth <id>/domain** command (see /cfg/vpn <id> /aaa/auth <id> Authentication Method Configuration on page 165).
type auto|get|post|web This command lets you view or configure the backend server's authentication type. When the link is created the first time, the VPN Gateway has automatically analyzed the web page's authentication type and set it to `auto` . If you keep this setting, the AVG will continue checking the web page's authentication type each time a remote user clicks the **iauto** link. To set a specific authentication type, use any of the **get, post** or **web** settings. • **auto**. Indicates that the VPN Gateway automatically analyzes the URL to determine the authentication type used on the backend server. • **get**. Used for backend servers providing form-based authentication, where the authentication form uses the GET method. • **post**. Used for backend servers providing form-based authentication, where the authentication form uses the POST method. • **web**. Used for backend web servers providing HTTP-based authentication, such as NTLM or basic (www-authenticate). The link automatically includes the user credentials provided on Portal logon as authentication headers. If the backend server requires a Windows domain (along with user name and password), the domain name specified with the **/cfg/vpn <id>/aaa/auth <id>/domain** command (see /cfg/vpn <id> /aaa/auth <id>

Command Syntax and Usage
Authentication Method Configuration on page 165) will automatically be included in the **iauto** link.
method https|https
Specifies the protocol used to access the backend server, that is, HTTP or HTTPS.
host
Specifies the backend server's IP address or host name, e.g. www.example.com.
path
Specifies the path to the desired web page, e.g. /login/login.asp. **Note:** The internal authentication database uses the path as one of the criteria by which it provides authentication credentials to a query. If you enter the path as **/Protected**, the internal database path will be / (that is, `root`), because **Protected** is treated as the filename. To treat **Protected** as a directory you must enter **/Protected/**. The iauto internal authentication database will then have **path=/Protected/** rather than /.
proxy on|off
By setting this command to **on**, the **iauto** link is configured for use with the HTTP Proxy applet. This means that the link will function properly if the user has previously clicked an HTTP Proxy link on the Portal's Home tab or started an HTTP Proxy session from the Portal's Advanced tab. **Note:** If the **iauto** link is configured for use with the HTTP Proxy applet (by setting this command to **on**), a HTTP Proxy session must have been started prior to clicking the `iauto` link. The default value is **off**. For more information about the HTTP Proxy applet (when invoked through the **proxy** link), see /cfg/vpn <id> /linkset <id> /link <id> Link Configuration on page 333.
mapping
Displayed when **type** is set to **auto, get** or **post**. Displays the Iauto Mapping menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /iauto/mapping Internal Auto-Logon Mapping Configuration on page 375.
cookies

Command Syntax and Usage	
	Displays the IAuto Cookies menu. To view menu options, see /cfg/vpn <id> /linkset <id> /link <id> /iauto/cookies Internal Auto-Logon Cookie Configuration on page 376.
mode	
	Some web servers providing basic, HTTP-based authentication (popup window with user name and password fields) require a domain name in addition to the user name to be inserted in the user name field. Example: User: <domain>\<user> Password: <password> If this is the case, the **mode** command lets you change the setting from **normal** to **add_domain**. The domain name added to the user name field will be the one specified for the relevant authentication method with the **/cfg/vpn <id>/aaa/auth <id>/domain** command.

/cfg/vpn <id> /linkset <id> /link <id> /iauto/mapping Internal Auto-Logon Mapping Configuration

```
[IAuto Mapping Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The Iauto Mapping menu is used to view or configure the values to be inserted for each field on a form-based authentication web page. When the `iauto` link is configured, the VPN Gateway automatically detects existing input fields on the specified web page and displays them in the CLI. You can either specify the desired values at that time or use the IAuto Mapping menu to specify or change these values later.

Table 195: Iauto Mapping Menu Options (/cfg/vpn/linkset/link/iauto/mapping)

Command Syntax and Usage	
list	
	Lists the currently configured mapping entries by index number.
del	
	Removes the mapping entry that is represented by the index number you specify. Use the **list** command to view all entries and related index numbers currently added to the list.
add	

Command Syntax and Usage
Lets you add mapping values for each input field on the form. • **key**. Represents an input field (= input name) on the form, e.g. **user**. • **value**. Tells the VPN Gateway what value to insert in the field, for example a macro, a specific text string or a combination of both. The <*var:user*> and <*var:password*> macros expand to the logged in Portal user's credentials. The <*var:domain*> macro expands to the domain name specified for the current authentication ID, using the **/cfg/vpn <id>/aaa/auth <id>/domain** command (see /cfg/vpn <id> /aaa/auth <id> Authentication Method Configuration on page 165).
insert
Lets you assign a specific index number to the mapping entry you add. The index number you specify must be in use. Mapping entries with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move
Lets you move a mapping entry up or down in the list. To view all mapping entries, use the **list** command.

/cfg/vpn <id> /linkset <id> /link <id> /iauto/cookies Internal Auto-Logon Cookie Configuration

```
[IAuto Cookies Menu]
list - Listall values
del  - Delete a value by number
add  - Add a new value
insert     - Inserta new value
move - Move a value by number
```

The Iauto Cookies menu is used to add the desired cookie strings, if the application requires that certain cookies are present when the GET request is made. The cookies are only sent for iauto links leading to a form.

Table 196: Iauto Mapping Menu Options (/cfg/vpn/linkset/link/iauto/cookies)

Command Syntax and Usage
list Lists the currently configured entries by index number.
del

Command Syntax and Usage
Removes the entry that is represented by the index number you specify. Use the **list** command to view all entries and related index numbers currently added to the list.
add
Lets you add the desired cookie strings as key/value. • **key**. Enter the key here, for example icaClientCode. • **value**. Enter the value here, e.g. 1.
insert
Lets you assign a specific index number to the entry you add. The index number you specify must be in use. Entries with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move
Lets you move an entry up or down in the list. To view all entries, use the **list** command.

/cfg/vpn <id>/sslclient Net Direct and SSL VPN Client Configuration

```
[SSL VPN Client Menu]
netdirect  - Enable Netdirect client access
caching    - Set allow caching of Netdirect client
ndbanner   - Set Netdirect banner text
ndlicense  - Set Netdirect license text
oslist     - Set Netdirect OSs
udpports   - Ports to use for encrypted UDP transport
rekeytraf  - Set rekey traffic limit
rekeytime  - Set rekey time limit
portalbind - Set Enable Netdirect to remain active after browser is closed
keepalive  - Set UDP Silent KeepAlive
recncttime - Set NetDirect connection retry time
idlecheck  - Set Terminate NetDirect client when idle
clampmss   - Adjust MSS field of TCP SYN to optimize packet sizes
splittun   - Set split tunnel mode
splitnets  - Networks for split tunnels
failover   - Configure VPN FailOver Servers
adv        - Advanced settings menu
mobility   - Mobility settings menu
tdiclient  - Enable TDI client access
tdioslist  - Set TDI client OSs
tdivsn     - Set TDI client minimum version
lspclient  - Enable LSP client access
lsposlist  - Set LSP client OSs
lspvsn     - Set LSP client minimum version
oldclients - Enable access for old (pre-6.0) TDI and LSP clients
xmlconfig  - Set XML client configuration
```

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). The SSL VPN client comes in two versions, the TDI client and the LSP client. For more information about these clients, see the "Net Direct" and "Transparent Mode" chapters respectively in the *Application Guide for VPN*.

Table 197: SSL VPN Client Menu Options (/cfg/vpn/sslclient)

Command Syntax and Usage
netdirect on|group|off Lets you specify whether or not remote users should be able to download/run the Net Direct client. • **on**: Net Direct is enabled. For the user to be able to download the Net Direct client, a Net Direct link must also be created on the Portal's Home tab. When set to **on**, the **caching, ndbanner, ndlicense, oslist, udpports, rekeytraf, rekeytime, idlecheck, clampmss, splittun, keepalive** and **splitnets** commands become visible. • **group**: Lets you specify on group level whether or not Net Direct usage should be allowed. Also see the **/cfg/vpn <id>/aaa/group <id>/ netdirect** command. • **off**: Net Direct is disabled. The default value is **off**.
caching on|off Lets you specify whether or not caching of Net Direct components on the client machine is allowed. This feature is only supported 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. The default value is **off**.
ndbanner <*banner text*> Lets you enter or paste the banner text to be displayed when the user starts the Net Direct client. If this command is ignored, the banner screen will not be displayed. The banner text screen will be displayed for the downloadable client as well as for the installed Net Direct client. Having entered/pasted the text, press ENTER and type three periods (...). Finally press ENTER once again.

Command Syntax and Usage
Below is an example of a banner text: `Welcome! You now have secure access to the intranet through Net Direct. Do not leave your computer unattended while connected!`
ndlicense <*license text*>
Lets you enter or paste a custom license text to be displayed in Net Direct's License agreement screen. The screen is displayed when Net Direct is started. This license text is not displayed for the installable Net Direct client. Having entered/pasted the text, press ENTER and type three periods (...). Finally press ENTER once again. **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. To print the default license text in the CLI (for copying), enter **cur ndlicense**. If you do not want the License agreement screen to be displayed at all, simply type three periods (...) and press ENTER. This will remove the default license text or any previously entered or pasted custom license text. **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.
oslist <*comma separated list of 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 list specified with this command, the Net Direct client is not allowed to connect to the VPN Gateway. Press TAB to view available options. Enter a comma separated of allowed OSs, e.g. **winxp,win2k** • **all**: All Net Direct client connections are allowed, irrespective of what OS the client runs on. • **unknown**: Net Direct clients running on an OS that cannot be identified (for example new OS versions) are allowed to connect. • **winxp**: Net Direct clients running on Windows XP are allowed to connect. • **win2k**: Net Direct clients running on Windows 2000 are allowed to connect. • **generic_win**: Net Direct clients running on any other Windows version are allowed to connect. • **mac**: Net Direct clients running on Mac OS X are allowed to connect. • **linux**: Net Direct clients running on Linux are allowed to connect. The default value is **all**.

Command Syntax and Usage
udpports
Lets you configure UDP ports to be used by the Net Direct client. The Net Direct client will use configured ports for sending encrypted UDP packets to the VPN Gateway. If this fails (due to for example firewalls between the client and the), the fallback is to use TCP. A range of at least two ports needs to be specified. The default port range is 5000-5001.
rekeytraf <*traffic in Kbytes*>
This setting does only apply to the Net Direct client. Sets the maximum traffic allowed before new session keys are exchanged between the Net Direct client and the VPN Gateway. If desired, you can choose this option instead of the **rekeytime** option (see below) or combine both. The default value is 0, which disables the service. This command is only available if the **netdirect** command is set to **on**.
rekeytime <*maximum time in seconds, minutes or hours*>
This setting does only apply to the Net Direct client. Sets the maximum lifetime of the single session key. The setting controls how often new session keys are exchanged between the Net Direct client and the VPN Gateway. Limiting the lifetime of a single key used to encrypt data is a way of increasing session security. 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 0s (0 seconds) disables the service. This command is only available if the **netdirect** command is set to **on**.
portalbind on|off
Lets you keep the Net Direct active even after the browser is closed. Valid portalbind values are as follows: • **on**: The Net Direct client closes when the browser is closed, or the user navigates to another page, or logs out from the portal. • **off**: The Net Direct client remains active when the browser is closed, or the user navigates to another page, or logs out from the portal. The default value is **on**. The portalbind 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 portalbind is off, the EACA mode must be disabled, or, if enabled, configure EACA as runonce mode.
idlecheck on|off

Command Syntax and Usage
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. **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. The default value is **on**.
keepalive <0-600>
Enables silent keepalives from Net Direct client. The keepalive value ranges from 0 to 600. The value 0 disables the keepalives and values other than 0 specify the interval of keepalive packets. The silent keepalive is sent from the client when the tunnel mode is UDP and are used to prevent intermediate NAPT routers from timing out the UDP ports. The default value is 0.
recncttime <0-600>
Sets the maximum timeout for reconnection if the Net Direct connectivity to the server is lost. This helps to restore the Net Direct session without user intervention. The value ranges from 1m (1 minute) to 60m (60 minutes); default value is 3m (3 minutes). The value 0m (0 minute) disables the service. This command is available only if the Net Direct is enabled.
clampmss
This parameter is used to prevent packet fragmentation for Net Direct traffic. • **on**: The AVG clamps the MSS (maximum segment size) of a TCP SYN packet to the MSS of the real interface. This way packet fragmentation does not occur for TCP traffic, which optimizes the performance. • **off**: The AVG does not perform MSS clamping. Large encrypted packets from the virtual interface that do not fit into a single packet when sent to the server will be subject to fragmentation. This will result in a slower connection. The default value is **on**.
splittun disabled|enabled|enabled_inverse| enabled_inverse_local
Lets you set the desired split tunnel mode for Net Direct traffic. Split tunneling allows network traffic to travel either through a tunnel to the VPN Gateway or directly to the Internet. • **disabled**. Tunnels all network traffic through the Net Direct client to the VPN Gateway. • **enabled**. Tunnels traffic to specified networks to the VPN Gateway (see the Split Nets menu on /cfg/vpn <id> /sslclient/splitnets Split Nets Configuration on page 385). All other network traffic goes through the computer's normal network interface.

Command Syntax and Usage
• **enabled_inverse**. Does not tunnel traffic to specified networks, that is, traffic goes through the computer's normal network interface. All other network traffic is tunneled through the Net Direct client to the VPN Gateway. • **enabled_inverse_local**. Does not tunnel traffic to directly connected networks or to specified networks. This will for example allow the remote user to print locally, even while tunneled to the VPN Gateway. All other network traffic is tunneled through the Net Direct client to the VPN Gateway. **Note:** The Mac OS X tunneling modes **enabled_inverse** and **disabled** do not tunnel the local net. The **enabled_inverse** mode is not supported on Linux. If the user is running Net Direct on Linux or Mac OS X and the split tunneling mode is not supported, the **enabled_inverse_local** mode will be used as fallback. The default value is **enabled_inverse_local**.
splitnets
Displays the SplitNets menu where you can configure the network ranges or IP addresses when **enabled, enabled_inverse** or **enabled_inverse_local** mode is selected with the **splittun** command. To view menu options, see /cfg/vpn <id> /sslclient/splitnets Split Nets Configuration on page 385.
failover
Displays Fail Over Menu. For more information about the menu options, see /cfg/vpn <id>/sslclient/failover Fail Over configuration on page 386.
adv on|off
Displays NetDirect Advanced Menu. For more information about the menu options, see /cfg/vpn <id>/sslclient/adv NetDirect Advanced configuration on page 387.
mobility
You can control the mobility by enabling or disabling mobility per VPN or per group and setting maximum roaming time. Client tries to connect immediately after detecting a link state change. Following enhancements are provided in mobility: • Enable/disable mobility per VPN or per group. • Set maximum roaming time per VPN or per group. • Client connects immediately on detecting a link state change. • Net Direct device remains in the UP state even when the physical link and Net Direct session is down. • Server ensures that when the client reconnects due to mobility, the IP address assigned to that client is not changed. • Configure a list of networks on which mobility is allowed. This is configured per VPN. When a client attempts due to mobility, the new IP address of the client is

Command Syntax and Usage
compared against this list and reconnection is allowed only if it is specified in the list. • Syslog messages are generated for roaming events. • Net Direct status monitor displays irrespective of mobility is enabled or not.
tdiclient on|off
Lets you specify whether or not remote users with the TDI client (version of the SSL VPN client) installed are allowed to connect to the VPN Gateway. • **on**: Remote users are allowed to connect to the VPN Gateway using the TDI client. When set to **on**, the **tdioslist** and **tdivsn** commands become visible (see below). • **off**: Remote users are not allowed to connect to the VPN Gateway using the TDI client. The default value is **off**.
tdioslist <*comma separated list of 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 list specified with this command, the TDI client is not allowed to connect to the VPN Gateway. Press TAB to view available options, that is, **all, unknown, winxp, win2k** and **generic_win**. Enter a comma separated list of allowed OSs, e.g. **winxp,win2k** • **all**: All TDI client connections are allowed, irrespective of what OS the client runs on. • **unknown**: TDI clients running on an OS that cannot be identified (for example new OS versions) are allowed to connect. • **winxp**: TDI clients running on Windows XP are allowed to connect. • **win2k**: TDI clients running on Windows 2000 are allowed to connect. • **generic_win**: TDI clients running on any other Windows version are allowed to connect. • integer representing OS ID, e.g. `12` : If a TDI client tries to connect with an unknown OS version and fails, the log will include details of the client's OS in the form of OS ID number and description. By entering the OS ID number here, client connection will be allowed. The default value is **all**.
tdivsn <*client version number*>
Lets you specify the minimum version of TDI clients that are allowed to connect to the VPN Gateway. When the TDI client tries to connect, it sends its version number to the AVG. Syntax example: `7.0.0.0`

Command Syntax and Usage
In the preceding example, TDI clients with version `7.0.0.0` or higher are allowed to connect.
`lspclient on|off`
Lets you specify whether or not remote users with the LSP client (version of the SSL VPN client) installed are allowed to connect to the VPN Gateway. • **`on`**: Remote users are allowed to connect to the VPN Gateway using the LSP client. When set to **`on`**, the **`lsposlist`** and **`lspvsn`** commands become visible (see below). • **`off`**: Remote users are not allowed to connect to the VPN Gateway using the LSP client. The default value is **`off`**.
`lsposlist` <*comma separated list of 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 list specified with this command, the LSP client is not allowed to connect to the VPN Gateway. Press TAB to view available options, that is, **`all, unknown, winxp, win2k, win98, winnt, winme`** and **`generic_win`**. Enter a comma separated list of allowed OSs, e.g. **`winxp,win2k`** • **`all`**: All LSP client connections are allowed, irrespective of what OS the client runs on. • **`unknown`**: LSP clients running on an OS that cannot be identified (for example new OS versions) are allowed to connect. • **`winxp`**: LSP clients running on Windows XP are allowed to connect. • **`win2k`**: LSP clients running on Windows 2000 are allowed to connect. • **`win98`**: LSP clients running on Windows 98 are allowed to connect. • **`winnt`**: LSP clients running on Windows NT are allowed to connect. • **`winme`**: LSP clients running on Windows ME are allowed to connect. • **`generic_win`**: LSP clients running on any other Windows version are allowed to connect. • integer representing OS ID, for example `12` : If an LSP client tries to connect with an unknown OS version and fails, the log will include details of the client's OS in the form of OS ID number and description. By entering the OS ID number here, client connection will be allowed. The default value is **`all`**.
`lspvsn` <*client version number*>
Lets you specify the minimum version of LSP clients that are allowed to connect to the VPN Gateway. When the LSP client tries to connect, it sends its version number to the AVG.

Command Syntax and Usage
Syntax example: `7.0.0.0` In the preceding example, LSP clients with version `7.0.0.0` or higher are allowed to connect.
oldclients true|false
Lets you specify whether or not old versions (released before AVG software version 7.0) of the SSL VPN client (TDI and LSP) are allowed to connect to the VPN Gateway. • **true**: Clients released before AVG software version 7.0 are allowed to connect. • **false**: Clients released before AVG software version 7.0 are not allowed to connect. The default value is **false**.
xmlconfig
This setting does only apply to the installed SSL VPN client (that is, the TDI and/or LSP client), not the Net Direct client. Lets you paste a ready-to-use configuration file in xml format. The xml file determines the behaviour of the installed SSL VPN client (not the Net Direct client), for example which domains and IP addresses should be routed through the VPN Gateway when the remote user tries to access a resource. To produce a configuration file, install the SSL VPN client, make the desired settings in the SSL VPN client and export the configuration file. Instructions can be found in the "Transparent Mode" chapter in the *Application Guide for VPN* and in the SSL VPN client's online help. Remote users can then download the configuration through the SSL VPN client's wizard. If no configuration file has been pasted using the **xmlconfig** command, a default configuration will be downloaded to the client instead. This configuration tunnels all traffic to the VPN Gateway.

/cfg/vpn <id> /sslclient/splitnets Split Nets Configuration

```
[SplitNets Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
```

The Split Nets menu is used to configure the network ranges or IP addresses to which traffic should be tunneled through the VPN Gateway.

Table 198: Split Nets Menu Options (/cfg/vpn/sslclient/splitnets)

Command Syntax and Usage
list
Lists configured entries by index number.
del
Deletes the desired entry by index number.
add *<network IP address> <network mask>*
Lets you add the desired network IP address(es). When the remote user tries to access a host whose IP address matches a network specified here, traffic is tunneled through the VPN Gateway.

/cfg/vpn <id>/sslclient/failover Fail Over configuration

```
[Fail Over Menu]
      list        - List all values
      del         - Delete a value by number
      add         - Add a new value
```

This menu is used to configure a list of alternate sites to connect if the primary site is inaccessible. When NDIC connects, it retrieves this list and stores it as part of the profile. NDIC refreshes the list on every connection. Later, if NDIC fails to connect to the primary site, it tries to connect to the alternate sites one by one.

Note:

- The alternate site list is not exposed to the end user and is not editable by the end user.
- Failover command is visible only when Net Direct is enabled.

Table 199: Client fail over menu options (/cfg/vpn/sslclient/failover)

Command syntax usage
list
Lists all the configured servers.
add
Adds a server to the list.
del
Deletes an entry by specifying an index to the list.

/cfg/vpn <id>/sslclient/adv NetDirect Advanced configuration

```
[NetDirect Advanced Menu]
      routemon   - Set route monitoring behaviour on netdirect client
      allowproxy - Set NetDirect proxy settings for splittun
```

The NetDirect Advanced Menu is used to ignore route table changes that do not affect Net Direct tunnel. If a user manually adds or deletes a route, which was set by the Net Direct device, system disconnects and reconnects table entries in the process. This works on Windows, Linux, MAC, and portal version of Net Direct.

Table 200: NetDirect Advanced Menu Options (/cfg/vpn/sslclient/adv)

Command usage syntax
routemon on|off Lets you to monitor the route behavior on Net Direct Client. Valid options are as follows: • on: Route table changes affects the Net Direct tunnel. • off : Route table changes does not affect the Net Direct tunnel. Default value is on.
allowproxy on|off The Net Direct does not change the browser proxy settings when split is enabled. Default value is off.

/cfg/vpn <id> /sslclient/mobility Mobility configuration

```
[Mobility Menu]
roaming - Enable mobility per VPN or per group
roamtime - Mobility Roamtime per VPN or per group
roamnets - Networks for roaming
```

Using this menu, you can have the control over the mobility by enabling or disabling mobility per VPN or per group and setting maximum roaming time. Client tries connecting immediately on detecting a link state change.

Table 201: Mobility menu options (/cfg/vpn/sslclient/mobility)

Command usage syntax
roaming [ena/dis/group]

Command usage syntax
Specifies if mobility is enabled or disabled per VPN or per group. Default value is ena.
roamtime [1min – 24 hours]
Specifies the maximum mobility roam time that needs to be set. 5 min is the default value.

/cfg/vpn <id> /sslclient/mobility/roamnets Roaming networks configuration

```
[Roamnets menu]
list – List all values
add -  Add a new value
del – Delete a value by a number
```

The Net Direct session remains in the UP state even when the physical link and Net Direct session is down. If a link is temporarily disconnected in client side, mobility media status notifications waits till maximum roaming time set. The maximum number of roamnets is 32.

Table 202: Roaming networks menu options (/cfg/vpn 1/sslclient/mobility/roamnets)

Command syntax usage
list
Lists all roaming networks.
add
Adds a roaming network.
del
Deletes a roaming network.

/cfg/vpn <id> /adv Advanced VPN Configuration

```
[Advanced Menu]

interface          - Set backend interface used by VPN
```

```
dns             - DNS Settings Menu

rsa             - RSA Servers

license         - VPN license allocation menu

log             - Set log settings

vpnadmin        - Allow administration of vpn

migration       - Set session migration mode

usepac          - Set PAC support in Java Applets
```

The Advanced menu mainly contains commands for Secure Service Partitioning, that is, the ability for Internet Service Providers (ISPs) to host multiple VPN customers in a cluster of VPN Gateways. This includes binding the current VPN to a specific VPN customer's network, specifying the VPN customer's DNS server, allocate licenses to the VPN and setting the rights for VPN administration.

The **`rsa, license`** and **`vpnadmin`** commands are only accessible if a Secure Service Partitioning license is loaded. For more information about this feature, see the "Secure Service Partitioning" chapter in the *Application Guide for VPN*.

Table 203: Advanced Menu Options (/cfg/vpn/adv)

Command Syntax and Usage
`interface` Lets you reference a previously created interface, mainly for use with the Secure Service Partitioning feature. This interface should be configured to process traffic relating to a specific VPN customer's private network. For example, it has its own default gateway routing the customer's backend traffic. To configure the interface, use the **`/cfg/sys/host #/interface`** command (see /cfg/sys/host <id> /interface <id> Interface Configuration on page 415). **Note:** A VPN can be bound to an interface even though Secure Service Partitioning is not used, for example to point out a "private side" default gateway used for the VPN-related "private side" traffic.
`cauth on|off` Lets you enable common (or shared) authentication for several VPNs, even if the VPNs are bound to specific interfaces. This ability can be used in a Secure Service

Command Syntax and Usage
Partitioning configuration, where the ISP wishes to use the same set of authentication servers for several end-customers. • **on**: Sets the AVG to use the default routing for authentication services. • **off**: Authentication requests will be routed through the referenced backend interface (see the **interface** command above) to an authentication server on the end-customer's private network. The **cauth** command is only visible if the VPN is bound to an interface with the **interface** command (see above). The default value is **off**.
cradacct on|off
Lets you enable common (or shared) RADIUS accounting for several VPNs, even if they are bound to specific interfaces. This ability can be used in a Secure Service Partitioning configuration, where the ISP wishes to share the same set of accounting servers for several end-customers. • **on**: Sets the AVG to use the default routing for accounting services. • **off**: Accounting requests will be routed through the referenced backend interface (see the **interface** command above) to an accounting server on the end-customer's private network. The **cradacct** command is only visible if the VPN is bound to an interface with the **interface** command (see above). The default value is **off**.
dns
Displays the DNS settings menu for the current VPN. To view menu options, see /cfg/vpn <id> /adv/dns DNS Settings Configuration on page 392.
rsa
Start a wizard for configuring an RSA server for the current VPN. When the wizard is completed, the VPN RSA Servers menu is displayed. To view menu options, see /cfg/vpn <id> /adv/rsa VPN RSA Servers Configuration on page 394. **Note:** The **rsa** command is only available if the Secure Service Partitioning license is loaded.
license
Displays the License Allocation menu for the current VPN. To view menu options, see /cfg/vpn <id> /adv/license License Allocation Configuration on page 395. **Note:** The **license** command is only available if the Secure Service Partitioning license is loaded.

Command Syntax and Usage
log <*options separated by a comma*>
Lets you select one or several options, each generating their own set of syslog messages including date, time, type of request, user, source IP address and requested destination. • **all**: Logs all following options, that is, **login, http, portal, reject**, and **socks**. • **login**: Logs Portal logins and logouts. • **http**: Logs HTTP requests made from the Portal. • **portal**: Logs other Portal operations, for example FTP and SMB file server access. • **reject**: Logs rejected requests. • **socks**: Logs SOCKS operations, that is, requests made using the Portal's Advanced tab features (for example Telnet sessions) and SSL VPN client requests. The default value is **login**
vpnadmin true|false
In a Secure Service Partitioning configuration, this command lets you decide whether or not remote administration of the current VPN should be allowed through the Browser-Based Management Interface (BBI). • **true**. The end-customer's VPN administrator can manage parts of the VPN (for example portal appearance, links and so on) through the BBI. To restrict VPN administration to specific users within the VPN end-customer's organization, use the **/cfg/vpn <id>/aaa/group <id>/vpnadmin** command (also available for extended profiles). To access the BBI, the VPN administrator should log in to the Portal and select **VPN Administration** on the **Tools** tab. • **false**. Administration of the VPN is restricted to the service provider (ISP). The default value is **false**. **Note:** The **vpnadmin** command is only available if the Secure Service Partitioning license is loaded. For more information about the Secure Service Partitioning feature, see the "Secure Service Partitioning" chapter in the *Application Guide for VPN*.
migration strict|loose
This command is used to control VPN session options. If the number of cluster nodes increases, then the session migration becomes expensive. Therefore, to have the control over this, strict and loose options are used. If a cluster contains less than 10 nodes, then strict mode is recommended.

Command Syntax and Usage
• **strict**: When set to strict mode, the session information is recorded in the master-master database. This mode slows down the login procedure and synchronizes the operation. • **loose**: When set to loose mode, only some of the information will be lost. This helps in less overhead to the system. The default value is **strict**.
usepac true|false
This command can be used to force the Port Forwarder and HTTP Proxy applets (available on the Portal's Advanced tab or configurable as Portal links) to ignore any automatic proxy configuration script (PAC file) in Internet Explorer. • **true**: The PAC file (if any) is used. • **false**: The PAC file is ignored. The default value is **true**.

/cfg/vpn <id> /adv/dns DNS Settings Configuration

```
[DNS Settings Menu]
search     - Set DNS search list
servers    - DNS servers menu
```

The DNS settings menu lets you specify a default domain list for the current VPN. If a Secure Service Partitioning license has been loaded, you can also specify local DNS servers to be used by the VPN.

Table 204: DNS Settings Menu Options (/cfg/vpn/adv/dns)

Command Syntax and Usage
search *<domain names, separated by comma>* Sets the search domains, which are automatically appended to the host names a remote user types in the various address fields on the web Portal (if a match is found). Example: If you specify the search domain example.com, a remote user can access the web page inside.example.com by typing **inside** in the URL field displayed on the Portal's Home tab. If you specify more than one domain name, separate the names with comma (,). The domains are searched in the order you specify them, and the search stops when a valid domain name is found. A maximum number of 120 domains are allowed, each with a maximum number of 64 characters.

Command Syntax and Usage
servers
Displays the DNS servers menu. To view menu options, see /cfg/vpn <id> /adv/dns/servers DNS Servers Configuration on page 393. **Note:** The **servers** command is only accessible if a Secure Service Partitioning license is loaded. For more information about the Secure Service Partitioning feature, see the "Secure Service Partitioning" chapter in the *Application Guide for VPN*.

/cfg/vpn <id> /adv/dns/servers DNS Servers Configuration

```
[DNS Servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The DNS servers menu is used to configure one or more DNS servers for the current VPN. This possibility is used together with the Secure Service Partitioning feature, to enable name resolution queries against the end-customers' private DNS servers.

If no DNS server is configured here, the system's global DNS server settings will be used (see the **/cfg/sys/dns/servers** command).

Table 205: DNS Servers Menu Options (/cfg/vpn/adv/dns/servers)

Command Syntax and Usage
list Displays all configured DNS servers by their index number and IP address.
del *<DNS server by index number>*
Removes the specified DNS server from the VPN. Use the **list** command to display the index numbers of all added DNS servers.
add *<IP address of DNS server>*
Adds a DNS server to the VPN. This DNS server will be used for name resolution queries adhering to the current VPN. You can add up to 3 DNS servers to the configuration.
insert *<index number to insert at> <IP address of DNS server to add>*

Command Syntax and Usage
Assigns a specific index number to the DNS server you add. The index number you specify must be in use. DNS servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves a DNS server up or down in the list of configured servers. The index numbers you specify must be in use. To view all DNS servers currently added to the VPN, use the **list** command.

/cfg/vpn <id> /adv/rsa VPN RSA Servers Configuration

```
[VPN RSA Servers 1 Menu]
rsaname    - Set RSA server symbolic name
import     - Import sdconf.rec file
rmnodesecr - Remove Node Secret
del  - Remove RSA server
```

The VPN RSA Servers menu includes commands to configure VPN-specific RSA servers. Note that there is also the option to configure global RSA servers using the **/cfg/sys/rsa** command. Irrespective of where the RSA servers are configured, all configured RSA servers (both VPN-specific and global) will be available for selection using the **/cfg/vpn <id>/aaa /auth <id>/rsa/rsaname** command.

Table 206: VPN RSA Servers Menu Options (/cfg/vpn/adv/rsa)

Command Syntax and Usage
rsaname Sets the symbolic name of the RSA server. This name should correspond to the name assigned to the authentication method using the **/cfg/vpn <id>/aaa/auth <id>/rsa/rsaname** command (see /cfg/vpn <id> /aaa/auth <id> /rsa RSA SecurID Configuration on page 203).
import <*protocol* [tftp|ftp|scp|sftp]> <*server host name or IP address*> <*file name on server*> <*FTP user name and password*>
Lets you import a copy of the **sdconf.rec** file from a TFTP/FTP/SCP/SFTP server. The **sdconf.rec** file is a configuration file that contains critical RSA ACE/Server information. Contact your RSA ACE/Server administrator to obtain the file and make it available on the desired TFTP/FTP/SCP/SFTP server.
rmnodesecr

Command Syntax and Usage
If needed, the RSA node secret can be removed using this command. Authentication will then fail until the **Node secret created** check box is unchecked in the **Edit Agent Host** window on the RSA server.
del
Deletes the current RSA server information.

/cfg/vpn <id> /adv/license License Allocation Configuration

```
[License allocation Menu]
ssl - Set number of ssl licenses allocated by this VPN
ipsec     - Set number of ipsec licenses allocated by this VPN
```

The License Allocation menu is used to allocate the desired number of concurrent SSL and IPsec users to the currently selected VPN.

A license is valid for a certain number of concurrent users, for example 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 (for example in a virtual hosting setup), the number of concurrent users in each VPN can be set by the operator. VPNs that have not been explicitly allocated a number of users will share the common pool of users.

Note:

The License Allocation menu is only accessible if a Secure Service Partitioning license has been loaded. For more information about the Secure Service Partitioning feature, see the "Secure Service Partitioning" chapter in the *Application Guide for VPN*.

Table 207: License Allocation Menu Options (/cfg/vpn/adv/license)

Command Syntax and Usage
ssl
Lets you specify the number of concurrent SSL users allocated to the current VPN. SSL is the protocol used for the secure tunnel when the remote user connects to the VPN through their browser, through the installed SSL VPN client or through Net Direct. If a user logs in through IPsec and there is no IPsec user license available, an SSL user license can instead be used (if available).
ipsec
Lets you specify the number of concurrent IPsec users allocated to the current VPN. IPsec is the protocol used for the secure tunnel when the remote user

Command Syntax and Usage
connects to the VPN through the IPsec VPN client (formerly the Contivity VPN client). If a user logs in through IPsec and there is no IPsec user license available, an SSL user license can instead be used (if available). **Note:** This command is not available if the VPN Gateway software is run on the ASA 310 or ASA 410 hardware platforms.

/cfg/ vpn <id>/spoclient SPO Client configuration

```
[SPO Client Menu]
      logoimport - Import logo banner image
      logofile   - Show installed logo file
      sysicon    - Import system tray icon image
      sysiconfil - Show installed sysicon file
      restorelog - Restores default Nortel logo
      restoresys - Restores default Nortel system tray icon
      bannertext - Set static banner text/licence/warning for users
      backupserv - Configure SPO Client backup servers
      software   - SPO Client Software Image Menu
      apps       - SPO Client Application Menu
      minver     - Set SPO Client software minimum version
      name       - Set SPO Client software name
```

Note:

Screen displays up to 10 letters of the menu name. To view the full menu name, type the menu name, and then press `<Tab>`.

The following table gives information on command syntax usage for the command `/cfg/vpn <id>/spoclient` .

Table 208: SPO management menu options (/cfg/vpn <id>/spoclient)

Command Syntax and Usage
logoimport Import logo banner image in gif format for SPO. The graphic logo image and the banner text (Terms and Conditions or License Agreement) are shared with portal. The protocols tftp/ftp/scp/sftp are used for transfer. Default value is tftp.
logofile Shows the logo image file name.

Command Syntax and Usage
sysicon
Lets you import system tray icon for SPO. The protocols, tftp/ftp/scp/sftp are used for transfer. Default value is tftp.
sysiconfile
Lets you import system tray icon file name for SPO.
restorelogo
Restores default Avaya logo for SPO.
restoresysicon
Restores default system tray icon for SPO.
bannertext
Sets the Terms and Conditions and License agreements for SPO users.
backupserver
Configures SPO VPN backup servers. For more information, see /cfg/ vpn <id>/spoclient/backupserver Backup Server configuration on page 397.
software
Lets you import SPO software image. AVG supports U3P, MSI and ISO image. For more information on this command, see /cfg/ vpn <id>/spoclient/software Software Image Menu on page 398.
apps
Imports user application. You can download user application to SPO device. AVG allows up to 50 applications to be configured. For more information on this command, see Table 210: Application (/cfg/ vpn <id>/spoclient/apps) on page 399.
minver
Sets minimum version of SPO client software supported by the server.
name
Sets SPO client software name.

/cfg/ vpn <id>/spoclient/backupserver Backup Server configuration

```
[Backup server Menu]
```

```
list      - List all values

del       - Delete a value by a number

add       - Add a new value
```

/cfg/ vpn <id>/spoclient/software Software Image Menu

```
[Software Image Menu]

iso       - Add CDROM iso image [FTP/TFTP/SFTP/SCP]

u3p       - Add USB U3 package [FTP/TFTP/SFTP/SCP]

msi       - Add generic USB Microsoft installer file [FTP/TFTP/SFTP/SCP]

list      - Lists all values.

del       - Delete [iso/u3p/msi]
```

Users can add the following software in the VPN Gateway:

- Third party software- Only zip files can be uploaded in the VPN Gateway.
- Software upgraded for SPO client - U3 package and MSI files can be uploaded in the VPN Gateway.

The following table gives the information on command syntax usage for the command /cfg/ vpn <id>/spoclient/software.

Table 209: Software Menu (/cfg/ vpn <id>/spoclient/software)

Command Syntax and Usage	
iso	
	Lets you import the ISO SPO software image through the protocols, FTP, TFTP, SFTP, or SCP.
u3p	
	Lets you import the U3P SPO software image through the protocols, FTP, TFTP, SFTP, or SCP.
msi	

Command Syntax and Usage	
	Lets you import the MSI SPO software image through the protocols, FTP, TFTP, SFTP, or SCP.
list	
	Lists SPO client software image directory.
del	
	Deletes the uploaded SPO software from AVG.

Note:

Importing or uploading image file using iso, u3p, or msi command does not require apply to commit.

/cfg/ vpn <id>/spoclient/apps SPO Client Application Menu

```
[SPO client Application 1 Menu]

name        - Set application name

version     - Set application version

software    - Add SPO application

del         - Delete a value
```

The following table gives the information on command syntax usage for the command /cfg/vpn <id>/spoclient/apps.

Table 210: Application (/cfg/ vpn <id>/spoclient/apps)

Command Syntax and Usage
name Displays the SPO application name.
version Displays the SPO application version.

Command Syntax and Usage
add
Lets you import the SPO application file through the protocols FTP/TFTP/SFTP/SCP.
del
Deletes the current SPO application from AVG.

/cfg/vpn <id> /syslog Syslog configuration

```
[syslog per vpn Menu]

list            - List all values

del             - Delete a value by number

add             - Add a new value

insert          - Insert a new list value

move            - Move a value by number
```

The syslog menu can be configured per VPN. All VPN specific syslog messages are sent to both the global syslog and the VPN syslog.

Note:

Per VPN syslog is available only with SSP license.

Table 211: syslog per vpn menu (/cfg/vpn/syslog)

Command Syntax and Usage
list
Displays all configured VPN by their index number, IP address, and facility number.
del
Removes the specified VPN syslog from the system configuration.
add

Command Syntax and Usage
Adds a VPN syslog to the system configuration.
insert
Assigns a specific index number to the VPN syslog you add. The index number you specify must be in use. VPN syslogs with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move
Moves a VPN syslog up or down in the list of configured servers. The index numbers you specify must be in use.

/cfg/vpn <id> /vdesktop Virtual desktop configuration

```
[Virtual desktop Menu]

ena             - enables virtual desktop

dis             - disables the virtual desktop

prelogon        - starts virtual desktop prior to logon

always          - uses virtual desktop always

force           set force virtual desktop before logging

switch          - switch between the desktops

secure          - secure file access

persist         - enables persist mode in vdesktop

filesep         - prevents users from seeing files

remdisk         - copies files

print           - print files
```

```
netshare        - share files

cryptlevel      - encryption level

timeout         - inactivity timeout

conncntrl       - Set connection control

mcd             - Malicious Code detection menu
```

This menu lets the administrator create a link to launch the virtual desktop. When a user clicks the virtual desktop link on the portal, the virtual desktop is launched. A browser is opened within virtual desktop where the user will be logged in automatically. A Tunnel Guard check is run and a portal matching the selected extended profiles is displayed.

Table 212: virtual desktop menu options (/cfg/vpn/<id>/vdesktop)

Command Syntax and Usage
ena Enable Virtual Desktop.
dis Disable Virtual Desktop. This is the default value.
group Allows group wise setting for virtual desktop. When set to group, prelogon and force options are hidden.
prelogon on|off When set to on, it allows user to start virtual desktop prior to logon.
always on|off When set to on, it forces the user to always use virtual desktop.
force on|off Set this option to launch portal inside virtual desktop. User will be forced to use virtual desktop for login.
switch on|off When set to on, it allows the user to switch between normal desktop and virtual desktop.
secure on|off When set to on, it allows the user to use only the default browser in vdesktop.

Command Syntax and Usage
persist on|off
When set to on, enables persistent mode on vdesktop.
filesep on|off
When set to on, prevents users from using or seeing the files that are on the normal desktop.
remdisk on|off
When set to on, permits users to copy files from vdesktop to removable disk.
print on|off
When set to on, prints files from vdesktop.
netshare on|off
When set to on, save files and map drives through windows SMB.
cryptlevel
Sets encryption level for vdesktop.
timeout
Sets inactivity timeout for vdesktop. The time should be entered in mins.
conncntrl<on/off>
Connection control acts as a firewall allowing only portal traffic from virtual desktop. Enabling this feature allows traffic to the portal IP address. Default value is off.
mcd
Displays the Malicious Code Detection menu. The Malicious Code Detection (MCD) includes malicious software like computer viruses, worms, trojan, and spyware. For menu options see /cfg/vpn <id>/vdesktop/mcd Malicious Code Detection on page 403.

/cfg/vpn <id>/vdesktop/mcd Malicious Code Detection

```
[MCD Menu]
      ena        - Enable Malware Detection
      dis        - Disable Malware Detection
      keylogger  - Set detect key loggers
      scrscrap   - Set detect screen scrappers
      acntcreate - Set disable creation of local machine accounts
      vkeyboard  - Virtual Keyboard
```

Using this menu, malware software can be detected.

Table 213: Malware menu /cfg/ vpn <id>/vdesktop/mcd

ena This option enables the virtual desktop option.
dis This option disables the virtual desktop option.
keylogger on|off This option enables the detection for key logger. Therefore this monitors every key stroke a user types on the key board. By default its value is off.
scrscrap on|off Screen scrappers usually ignores the binary data and formatting that makes the desired text less visible. This option enables detection of screen scrappers. By default its value is off.
acntcreate on|off This option disables the local machine accounts. Default value is off.
vkeyboard on|off Displays the Virtual Keyboard menu. For more information about options, see /cfg/vpn <id>/vdesktop/mcd/vkeyboard Virtual Keyboard Configuration on page 404.

/cfg/vpn <id>/vdesktop/mcd/vkeyboard Virtual Keyboard Configuration

```
[VirtualKeyboard Menu]
      ena         - Enable Virtual Keyboard
      dis         - Disable Virtual Keyboard
      trigger     - Trigger
```

The Virtual Keyboard Menu configures the Symantec On-Demand Protection Agent (SODA) virtual keyboard. Symantec On Demand Protection (SODP) integrates the Malicious Code Detection (MCD) and Avaya VPN Gateway (AVG) logon. 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 it forces the PC to virtual desktop or keyboard mode. The SODP version is upgraded from version 3.1.1 to 3.1.3, this version is used in AVG 9.0.

Table 214: Virtual Keyboard Options (/cfg/vpn/vdesktop/mcd/vkeyboard)

Command Usage and Syntax
ena Enables the virtual keyboard.
dis Deletes the virtual keyboard.
trigger

Command Usage and Syntax
Displays the Trigger menu. For more informations about options, see /cfg/vpn <id>/vdesktop/mcd/vkeyboard/trigger Virtual Keyboard Trigger Configuration on page 405.

/cfg/vpn <id>/vdesktop/mcd/vkeyboard/trigger Virtual Keyboard Trigger Configuration

```
[Trigger 1 Menu]
      name        - Set trigger name
      type        - Set Trigger type
      value       - Set Trigger value
      vkonoff     - Set Virtual Keyboard OnOff
      delete      - Remove Trigger
```

Use the Virtual Keyboard Trigger Menu to create triggers and configure the virtual keyboard.

Table 215: Trigger Menu options (/cfg/vpn/vdesktop/mcd/vkeyboard/trigger)

Command Usage and Syntax
name Sets the trigger name.
type Sets the trigger type.
value Sets the trigger value.
vkonoff Sets trigger action.
delete Removes the trigger.

/cfg/vpn <id>/syslog Syslog VPN configuration

```
[Syslog Per VPN Menu]

list            - List all values

del             - Delete a value by number

add             - Add a new value
```

```
insert          - Insert a new value

move            - Move a value by number
```

Using this menu, syslog can be configured per VPN. All VPN specific syslog messages are sent to both the global syslog and the VPN syslog.

Note:

Per syslog VPN is available only with SSP license.

Table 216: Syslog Per VPN Menu (/cfg/ vpn/syslog)

Command usage syntax
list Displays all configured VPN by their index number, IP address, and facility number.
del <index number>
Removes the specified VPN syslog from the system configuration. Use the list command to display the index numbers of all added VPN syslog.
add <IP address of VPN syslog><local facility number>
Adds a VPN syslog to the system configuration. When adding a VPN syslog you will be prompted for both the IP address and the local facility number. The local facility number can be used to uniquely identify syslog entries.
insert<index number to insert at><IP address of vpn syslog to add><local facility number>
Assigns a specific index number to the VPN syslog you add. The index number you specify must be in use. VPN syslogs with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
insert<index number to move><destination index number>
Moves a VPN syslog up or down in the list of configured servers. The index numbers you specify must be in use. To view all VPN syslogs currently added to the system configuration, use the list command

cfg/vpn <id>/sslclient/mobility Mobility configuration

```
[Mobility Menu] roaming - Enable mobility per VPN or per group roamtime -
Mobility Roamtime per VPN or per group
```

You can control the mobility by enabling or disabling mobility per VPN or per group and setting maximum roaming time. Client tries connecting immediately on detecting a link state change. This can be done using the command cfg/vpn <id>/sslclient/mobility.

Table 217: Mobility Menu (cfg/vpn/sslclient/mobility)

Command usage syntax
roaming [ena/dis/group] Specifies if mobility is enabled or disabled per VPN or per group.
roamtime [1min – 24 hours] Specifies the maximum mobility roam time that needs to be set. Default is 5 mins.

Note:

Only roaming and roamtime can be configured on group basis.

cfg/vpn <id>/sslclient/mobility/roamnets Mobility roaming networks

```
[roamnets menu]
list  - List all values
add   -  Add a new value
del   - Delete a value by a number
```

The Net Direct session remains in the UP state even when the physical link and Net Direct session is down. If a link is temporarily disconnected in client side, mobility media status notifications waits till maximum roaming time set. The maximum number of roamnets is 32.

Table 218: Mobility Menu (cfg/vpn <id>/sslclient/mobility)

Command usage syntax
list

Command usage syntax
Lists all roaming networks.
add
Adds a roaming network
del
Deletes a roaming network.

/cfg/sys System Configuration

```
[System Menu]
mip   - Set management IP (MIP) address
host - iSD host menu
routes      - Routes menu
time - Date and time menu
dns   - DNS settings
rsa   - RSA Servers
syslog      - Syslog servers menu
accesslist - Access list menu
adm   - Administrative applications menu
user - User Access Control menu
distrace    - Disable tracing with tcpdump/ssldump
```

The System menu is used for configuring system-wide parameters on a per cluster basis.

Table 219: System Menu Options (/cfg/sys)

Command Syntax and Usage
mip <*Management IP address*> Sets the Management IP (MIP) address. The MIP address identifies the cluster, and each MIP address must be unique on the network. For more information about clusters and MIP addresses, see the "Initial Setup" chapter in the *User's Guide*.
host Displays the iSD Host menu. To view menu options, see /cfg/sys/host <id> iSD Host Configuration on page 410.
routes Displays the Routes menu. To view menu options see /cfg/sys/routes Cluster Wide Routes Configuration on page 419.
time Displays the Date and Time menu. To view menu options, see /cfg/sys/time Date and Time Configuration on page 420.

Command Syntax and Usage
dns
Displays the DNS Settings menu. To view menu options, see /cfg/sys/dns DNS Settings Configuration on page 421.
rsa
Displays the RSA Servers menu. To view menu options, see /cfg/sys/rsa RSA Server Configuration on page 424.
syslog
Displays the Syslog Servers menu. To view menu options, see /cfg/sys/syslog Syslog Servers Configuration on page 425.
accesslist
Displays the Access List menu. To view menu options, see /cfg/sys/accesslist System Access Configuration on page 426.
adm
Displays the Administrative Applications menu. To view menu options, see /cfg/sys/adm Administrative Applications Configuration on page 427.
user
Displays the User menu. To view the options, see /cfg/sys/user User Access Configuration on page 445.
distrace
Permanently disables the usage of the **ssldump** and **tcpdump** commands in the Trace menu (**/cfg/ssl/server #/trace/ssldump|tcpdump**). This command is used to improve security and cannot be reversed by other means than a boot install.

/cfg/sys/host <id> iSD Host Configuration

```
>> Main# /cfg/sys/host 1/

------------------------------------------------------------
[Cluster Host 1 Menu]
      type       - Set type of the host
      ip         - Set IP address
      sysName    - Set sysName
      sysLocatio - Set sysLocation
      license    - Set License
      gateway    - Set default gateway address
      routes     - Routes menu
      ipsec      - Host IPsec menu
      interface  - host interface menu
      port       - host port configuration menu
      ports      - Display physical ports
      hwplatform - Display hardware platform
      halt       - Halt the host
      reboot     - Reboot the host
      delete     - Remove Cluster Host
```

The iSD Host menu is used for configuring basic TCP/IP properties for a particular VPN Gateway (iSD) in a cluster, as well as setting the VPN Gateway type to either master or slave. You can also halt, reboot or delete a VPN Gateway remotely through the iSD Host menu. To view the host number, type, and IP address for each VPN Gateway in the cluster, use the **/cfg/sys/host #/cur** command.

Table 220: iSD Host Menu Options (/cfg/sys/host)

Command Syntax and Usage
type master|slave Defines the currently selected VPN Gateway (host) as a master or slave. When installing a VPN Gateway in a new cluster (by selecting new in the Setup menu), it is automatically configured as master. When adding up to three additional VPN Gateways to the same cluster (by selecting join in the Setup menu), you are provided with the option to configure them as either master or slave. The default setting, however, for up to three additional VPN Gateways in one given cluster is master. This means that in a cluster containing four VPN Gateways, all four are configured as masters provided you accepted the default settings during the initial setup. When adding one or more VPN Gateways to a cluster that already contains four master AVGs, the added AVGs are automatically configured as slaves (without the option to change this during the initial setup).

Command Syntax and Usage
The AVG software supports clustering over multiple subnets. If more than one VPN Gateway is required and the AVG you wish to join to the cluster is installed in a different subnet, the new VPN Gateway must be configured as a slave. Master AVGs cannot exist on different intranet subnets. Normally, you will only need to change the **type** configuration when you have removed one or more master VPN Gateways in a cluster, in which there are also AVGs configured as slaves. In this case, you may want to promote one of the slaves to become a master. Depending on the total number of AVGs in a cluster and the desired level of redundancy, it is recommended that 2-4 AVGs are configured as masters. To view the status and current master/slave configuration of the VPN Gateways in a cluster, use the **/info/isdlist** command. To view the host number of each AVG in a cluster, use the **/cfg/sys/cur** command.
sysName Assigns an administratively-assigned name to the managed AVG host. Can be used when managing the AVG through SNMP (also see /cfg/sys/adm/snmp SNMP Management Configuration on page 429).
sysLocatio Adds a description of the physical location of the managed AVG host. Can be used when managing the AVG through SNMP (also see /cfg/sys/adm/snmp SNMP Management Configuration on page 429).
ip < AVG host IP address> Sets the host IP address of the currently selected VPN Gateway (host). Changing the IP address of a specific VPN Gateway does not affect the Management IP address (which defines the cluster itself, and not an individual VPN Gateway). A change of host IP address using this command always applies to a host on interface 1. You cannot change the host IP address on more than one AVG host at a time. If you want to move the management network to some other IP address space, you first have to delete all AVGs but one of the masters from the cluster. Then change the IP address of the master and rejoin all other AVGs. Note that you will be logged out when you apply the new IP address.
license Lets you paste the license key for the type of license you have purchased. Available licenses are: • SSL (Portal, Net Direct and SSL VPN client access). Available for 50, 100, 250, 500, 1000 and 2000 users. • IPsec (IPsec VPN client access). Available for 250, 500 and 1000 users. • TPS (transactions per second). Available for 300 TPS and 1000 TPS. No license is required for hardware platforms.

Command Syntax and Usage
• PortalGuard. Enables SSL acceleration of existing Portal (see the **/cfg/vpn <id> /server/portal/authentica** command. • Secure Service Partitioning. Enables Internet Service Providers (ISPs) to host multiple VPN customers in an AVG cluster. To obtain a license key, find out the MAC address of the VPN Gateway(s) on which you wish to install the license, using the **/info/local** command. Next, contact Avaya Support, provide the MAC address and you will be given the license key for the desired license type. **Note:** When pasting the license key, include the BEGIN LICENSE and END LICENSE lines.
gateway Sets the default gateway address of the currently selected VPN Gateway. This setting also implicitly determines the public interface in a two-armed configuration (or any configuration using more than one interface). The assumption is that the interface used to reach the default gateway is the public one, because the default gateway needs to be used to reach the clients on the Internet. When the AVG cluster is used for Secure Service Partitioning (hosting of multiple VPN end-customers), a default gateway should be specified for each dedicated VPN interface. See the **/cfg/sys/host #/interface/gateway** command on /cfg/sys/host <id> /interface <id> Interface Configuration on page 415. **Note:** A default gateway can be specified for a VPN interface (even though Secure Service Partitioning is not used) to point out a "private side" default gateway used for the VPN-related "private side" traffic.
routes Displays the Host Routes menu. To view menu options, see /cfg/sys/host <id> /routes Host Routes Configuration on page 414.
IPsec Displays the IPsec logins re-direction status.
interface *<iSD host interface number>* Displays the Host Interface menu. To view menu options, see /cfg/sys/host <id> /interface <id> Interface Configuration on page 415.
port Displays the Host Port menu. To view menu options, see /cfg/sys/host <id> /port <number> Host Ethernet Port Configuration on page 418.
ports

Command Syntax and Usage
Lists the number of physical ports on the selected VPN Gateway. If there are more than one physical port, the ports that can exist on the same network (for failover or trunking) are grouped together, separated by comma (,). A port that cannot exist on the same network as other listed ports will appear after a colon (:). Example output of the command: **`Ports = 1, 2 : 3`**
`hwplatform` Displays the hardware platform that the selected VPN Gateway is using.
`halt` Stops the currently selected VPN Gateway. Always use this command before turning off the device. If the VPN Gateway you want to halt has become isolated from the cluster, you will receive an error message when performing the **`halt`** command. You can then try logging in to the VPN Gateway through a console connection (or a Telnet or SSH connection to the AVG 's individually assigned IP address) and use the **`halt`** command in the Boot menu (**`/boot/halt`**).
`reboot` Reboots the currently selected VPN Gateway. If the VPN Gateway you want to reboot has become isolated from the cluster, you will receive an error message when performing the **`reboot`** command. You can then try logging in to the VPN Gateway through a console connection (or a Telnet or SSH connection to the AVG 's individually assigned IP address) and use the **`reboot`** command in the Boot menu (**`/boot/reboot`**).
`delete` Removes the currently selected VPN Gateway "cleanly" from the cluster, and resets the removed VPN Gateway to its factory default configuration. Other VPN Gateways (hosts) in the cluster are unaffected. To ensure that you remove the intended VPN Gateway, view the current settings by using the **`cur`** command. To view the host number, AVG type (master or slave), and IP address for all VPN Gateways in a cluster, use the **`/cfg/sys/cur`** command. After having removed a VPN Gateway from the cluster, you can only access the device through a console connection. Log in as the `admin` user with the `admin` password to enter the Setup menu. **Note:** You cannot delete a VPN Gateway that is included in the cluster configuration of other AVGs if the VPN Gateway you want to delete is the only machine in the cluster with the status up. If that is the case you will receive an error message when performing the **`delete`** command. To delete a VPN Gateway from the cluster while all the other AVG cluster members are down, log in to the VPN Gateway through a console connection (or through a Telnet or SSH connection using the AVG 's individually assigned IP address) and use the **`delete`** command in the Boot menu (**`/boot/delete`**). After having deleted the VPN Gateway using the **`/boot/delete`** command, and the remaining cluster members have regained the status up, you should also connect to the MIP

Command Syntax and Usage
address through Telnet or SSH and delete the VPN Gateway from the cluster configuration by using the **delete** command in the iSD Host menu. **Note:** If you are using the ASA 310-FIPS model and you want to reset the HSM cards when removing the ASA FIPS host from the cluster, you must use the **/boot/delete** command. For more information about resetting the HSM cards, see the "Resetting.HSM Cards on the ASA 310-FIPS" section in the "Troubleshooting the AVG " chapter in the *User's Guide*.

/cfg/sys/host <id> /routes Host Routes Configuration

```
[Host Routes Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
```

The Routes menu is used for managing static routes for a specific host when more than one interface is configured. To configure static routes on a cluster-wide level, use the **/cfg/sys/routes** command. To configure static routes for a specific interface, use the **/cfg/sys/host #/interface #/routes** command.

Table 221: Routes Menu Options (/cfg/sys/host/routes)

Command Syntax and Usage
list Lists all configured static routes by their index number and IP address information.
del <*static route by index number*>
Removes the specified static route from the host configuration. Use the **list** command to display the index numbers of all added static routes.
add <*destination IP address*> <*subnet mask*> <*gateway IP address*>
Adds a static route to the host configuration. Specify the destination IP address, the subnet mask, and the gateway IP address.

/cfg/sys/host <id> /interface <id> Interface Configuration

```
[Host Interface 1 Menu]
ip    - Set IP address
netmask     - Set network mask
gateway     - Set default gateway address
routes      - Routes menu
vlanid      - Set VLAN tag id
mode - Set mode
ports- Interface ports menu
primary     - Set primary port
delete      - Remove Host Interface
```

The Interface menu is used for configuring an IP interface and assigning 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.

To configure a new interface (in addition to the default Interface 1), enter an unused interface index number. To change the configuration of an existing interface, enter the corresponding interface index number. To get an overview of all configured interfaces, use the **/cfg/sys/host #/cur interface** command.

Table 222: Host Interface Menu Options (/cfg/sys/host/interface)

Command Syntax and Usage
ip <*network IP address*> Sets the network address for the currently selected interface.
netmask <*subnet mask*> Sets the subnet mask for the currently selected interface.
gateway <*IP address*> Sets the default gateway address to be used by this particular interface. The gateway will only be used for "private side" traffic, (for example decrypted traffic bound for the intranet, requests to private authentication servers and DNS servers), and only for VPNs that point to this interface (using the **/cfg/vpn <id>/adv/interface** command). If no VPN points to this interface, the gateway specified here will be ignored. When the AVG cluster is used for Secure Service Partitioning (hosting of multiple VPN customers), a default gateway should be specified here for each dedicated VPN interface.
routes Displays the Routes menu. To view menu options, see /cfg/sys/host <id> /interface <id> /routes Interface Routes Configuration on page 416.

Command Syntax and Usage
vlanid
Sets the desired VLAN tag id. Used if packets received by the currently selected interface are tagged with a specific VLAN tag id, for example by a connected switch.
mode failover|trunking
Specifies the mode of operation for the port numbers you have configured for use in a single IP interface. • **failover:** In this 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 selecting failover mode, you are also provided with the option to specify a primary port. • **trunking:** In this mode, active links are sustained on all configured ports simultaneously to increase network throughput. The default mode is **failover**.
ports
Displays the Interface Ports menu. To view menu options, see /cfg/sys/host <id> / interface <id> /ports Interface Ports Configuration on page 417.
primary <*primary port by number*>
Specifies which of the configured ports that should always be used as the primary port, on which the active link is set up. 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). The default value indicates 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, and the mode is set to **failover**.
delete
Removes the current interface from the system configuration.

/cfg/sys/host <id> /interface <id> /routes Interface Routes Configuration

```
[Host Interface Routes Menu]
```

```
list       - List all values
del  - Delete a value by number
add  - Add a new value
```

The Host Interface Routes menu is used to configure static routes for the current interface, if required.

Any routes specified here will only be used for "private side" traffic, (for example decrypted traffic bound for the intranet, requests to private authentication servers and DNS servers), and only for VPNs that point to this interface (using the **/cfg/vpn <id>/adv/interface**command).

If no VPN points to this interface, routes specified here will be ignored.

Table 223: Interface Routes Menu Options (/cfg/sys/host/interface/routes)

Command Syntax and Usage
list Displays all routes that are assigned to the currently selected interface.
del <*route by index number*> Removes the specified route, currently assigned to the selected interface.
add <*destination address*> <*network mask*> <*gateway address*> Adds a route to be used by the currently selected interface.

/cfg/sys/host <id> /interface <id> /ports Interface Ports Configuration

```
[Interface Ports Menu]
list - List all values
del  - Delete a value by value
add  - Add a new value
```

The Interface Ports menu is used for listing the ports currently assigned to the selected interface. The menu is also used for adding or deleting ports to/from the selected interface. The interface ports configuration is only applied to those AVG devices in the cluster that are equipped with the physical port represented by the port number you specify.

To view the available port numbers on a particular AVG device in the cluster, use the **/cfg/sys/host #/ports** command. This command also provides information about which port numbers that can be assigned to the same interface for failover or trunking.

Table 224: Interface Ports Menu Options (/cfg/sys/host/interface/ports)

Command Syntax and Usage
list Displays all ports that are assigned to the currently selected interface.
del *<port by number>* Removes the specified port, currently assigned to the selected interface.
add *<port by number>* Adds a port to be used in the currently selected interface.

cfg/sys/host id/ipsec

```
[Host IPsec Menu]
      dfbit      - Set IPsec DF bit
      blocklogin - Block IPsec logins
```

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.

Table 225: IPsec Menu options (/cfg/sys/host <id>/ipsec)

Command Syntax and Usage
dfbit <policy> Sets the IPsec DF bit policy as copy or reset.
blocklogin <boolean> Sets the blocklogin state as on or off.

/cfg/sys/host <id> /port <number> Host Ethernet Port Configuration

```
[Host Port 1 Menu]
autoneg    - Set autonegotiation
speed- Set Speed
mode - Set full or half duplex mode
```

The Host Port menu is used for specifying the properties of a port, with reference to autonegotiation, speed and mode.

Table 226: Host Port Menu Options (/cfg/sys/host/port)

Command Syntax and Usage
autoneg on|off Sets Ethernet autonegotiation to **on** or **off** for the currently selected host and NIC port. The default and recommended setting is **on**. Make sure that the device the port is connected to uses the same Ethernet autonegotiation settings. **Note:** When autonegotiation is set to **on**, the settings for speed and (duplex) mode are ignored.
speed <*port speed in Mbits per second [10|100|1000]*> Sets the speed for the currently selected host and NIC port when autonegotiation is set to **off**.
mode full|half Sets the duplex mode for the currently selected host and NIC port when autonegotiation is set to **off**. The default duplex mode is set to **full**.

/cfg/sys/routes Cluster Wide Routes Configuration

```
[Routes Menu]
list - List all values
del  - Delete a value by number
add        - Add a new value
```

The Routes menu is used for managing static routes on a cluster-wide level when more than one interface is configured. To configure static routes for a specific host, use the **/cfg/sys/host #/routes** command. To configure static routes for a specific interface, use the **/cfg/sys/host #/interface #/routes** command.

Table 227: Routes Menu Options (/cfg/sys/routes)

Command Syntax and Usage
list Lists all configured static routes by their index number and IP address information.

Command Syntax and Usage
del <*static route by index number*>
Removes the specified static route from the system configuration. Use the **list** command to display the index numbers of all added static routes.
add <*destination IP address*> <*subnet mask*> <*gateway IP address*>
Adds a static route to the system configuration. Specify the destination IP address, the subnet mask, and the gateway IP address.

/cfg/sys/time Date and Time Configuration

```
[Date and Time Menu]
date - Set system date
time - Set system time
tzone- Set Timezone
ntp  - Configure NTP servers
```

The Date and Time menu is used for setting system date and system time. It is also used for changing the time zone, and for accessing the NTP Servers menu.

Table 228: Date and Time Menu Options (/cfg/sys/time)

Command Syntax and Usage
date <*date (YYYY-MM-DD)*>
Sets the system date according to the specified format.
time <*time (HH:MM:SS)*>
Sets the system time using a 24-hour clock format.
tzone
Sets the time zone. Select a continent or ocean, a country, and a region (if applicable).
ntp
Displays the NTP Servers menu. To view menu options, see /cfg/sys/time/ntp NTP Servers Configuration on page 421.

/cfg/sys/time/ntp NTP Servers Configuration

```
[NTP Servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
```

The NTP Servers menu enables you to list the configured NTP servers, delete an NTP server, or add a new NTP server to the configuration.

Table 229: NTP Servers Menu Options (/cfg/sys/time/ntp)

Command Syntax and Usage
list Lists all configured NTP servers by their index number and IP address.
del <*NTP server by index number*> Removes the specified NTP server from the system configuration. Use the **list** command to display the index numbers of all added NTP servers.
add <*IP address of NTP server*> Adds an NTP server to the system configuration. The NTP server you add is used by the NTP client on the VPN Gateway to synchronize its clock. NTP should have access to a number of servers (at least three) to compensate for any discrepancies in the servers.

/cfg/sys/dns DNS Settings Configuration

```
[DNS Settings Menu]
servers    - DNS servers menu
cachesize  - Set Local DNS cache size
retransmit - Set DNS Retransmit interval timer
count- Set DNS Retransmit counter
ttl  - Set Max TTL
health     - Set Health check interval
hdown- Set Health check down counter
hup  - Set Health check up counter
```

The DNS settings menu lets you access the DNS servers menu, where one or several global DNS servers can be added to the AVG cluster. The DNS settings menu also includes commands for fine tuning the DNS settings.

When using the Secure Service Partitioning feature, use this menu to add global DNS servers for your AVG cluster. To add private DNS servers, specific to different VPNs, use the **/cfg/vpn <id>/adv/dns/servers** command.

Table 230: DNS Settings Menu Options (/cfg/sys/dns)

Command Syntax and Usage
servers Displays the DNS servers menu. To view menu options, see /cfg/sys/dns/servers DNS Servers Configuration on page 423.
cachesize <*number of DNS entries*> Sets the maximum number of DNS entries in the local DNS cache. The default DNS cache size is 1000 entries.
retransmit <*value in seconds*> Sets the interval for retransmitting a DNS query. The default retransmit value is 2 seconds.
count <*integer value*> Sets the maximum number of times a DNS query is retransmitted. The default value is 3.
ttl <*integer value*> Sets the maximum Time-To-Live for a DNS entry in the cache. To specify a value in minutes, hours or days, enter an integer directly followed by the letter **m, h,** or **d,** for example **2h30m**. If you enter an integer not followed by one of these letters, seconds is implied. The default TTL value is 3 hours (3h).
health <*value in seconds*> Sets the DNS server health check interval. The VPN Gateway will perform a DNS query to each of the DNS servers added to the system configuration at the specified interval to determine the health check status. The default health check interval is set to 10 seconds (10s).
hdown Sets the number of times a DNS server health check can time out before the VPN Gateway determines the DNS server as down. The default health check down counter is set to 2.
hup Sets the number of times a DNS server health check returns a positive response before the VPN Gateway determines the DNS server as up. The default health check up counter is set to 2.

/cfg/sys/dns/servers DNS Servers Configuration

```
[DNS Servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The DNS Servers menu enables you to list the configured DNS servers, delete a DNS server, or add a new DNS server to the configuration.

Table 231: DNS Servers Menu Options (/cfg/sys/dns/servers)

Command Syntax and Usage
list Displays all configured DNS servers by their index number and IP address.
del <*DNS server by index number*>
Removes the specified DNS server from the system configuration. Use the **list** command to display the index numbers of all added DNS servers.
add <*IP address of DNS server*>
Adds a DNS server to the system configuration. The DNS servers you add will be used for all name resolution queries performed in the AVG cluster. You can add up to 3 DNS servers to the configuration.
insert <*index number to insert at*> <*IP address of DNS server to add*>
Assigns a specific index number to the DNS server you add. The index number you specify must be in use. DNS servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>
Moves a DNS server up or down in the list of configured servers. The index numbers you specify must be in use. To view all DNS servers currently added to the system configuration, use the **list** command.

/cfg/sys/rsa RSA Server Configuration

```
[RSA Servers 1 Menu]
rsaname    - Set RSA server symbolic name
import     - Import sdconf.rec file
rmnodesecr - Remove Node Secret
del  - Remove RSA server
```

The RSA Servers menu lets you configure the symbolic name for the RSA server and import the **sdconf.rec** configuration file. Note that there is also the option to configure VPN-specific RSA servers using the **/cfg/vpn <id>/adv/rsa** command. Irrespective of where the RSA servers are configured, all configured RSA servers (both VPN-specific and global) will be available for selection using the **/cfg/vpn <id>/aaa/auth <id>/rsa/rsaname** command.

Table 232: RSA Servers Menu Options (/cfg/sys/rsa)

Command Syntax and Usage
rsaname Sets the symbolic name of the RSA server. This name should correspond to the name assigned to the authentication method using the **/cfg/vpn <id>/aaa/auth <id>/rsa/rsaname** command (see /cfg/vpn <id> /aaa/auth <id> /rsa RSA SecurID Configuration on page 203).
import *<protocol [tftp|ftp|scp|sftp]> <server host name or IP address> <file name on server> <FTP user name and password>* Lets you import a copy of the **sdconf.rec** file from a TFTP/FTP/SCP/SFTP server. The **sdconf.rec** file is a configuration file that contains critical RSA ACE/Server information. Contact your RSA ACE/Server administrator to obtain the file and make it available on the desired TFTP/FTP/SCP/SFTP server.
rmnodesecr If needed, the RSA node secret can be removed using this command. Authentication will then fail until the **Node secret created** check box is unchecked in the **Edit Agent Host** window on the RSA server.
del Deletes the current RSA server information.

/cfg/sys/syslog Syslog Servers Configuration

```
[Syslog Servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The Syslog Servers menu is used to configure syslog servers. The AVG software can send log messages to the specified syslog hosts. For a list of all log messages that the VPN Gateway can send to a syslog server, see Appendix C, Syslog Messages, in the *User's Guide*.

Table 233: Syslog Servers Configuration Menu Options (/cfg/sys/syslog)

Command Syntax and Usage
list Displays all configured syslog servers by their index number, IP address, and facility number.
del <*index number*> Removes the specified syslog server from the system configuration. Use the **list** command to display the index numbers of all added syslog servers.
add <*IP address of syslog server*> <*local facility number*> Adds a syslog server to the system configuration. When adding a syslog server you will be prompted for both the IP address and the local facility number. The local facility number can be used to uniquely identify syslog entries. For more information, see the manual page for **syslog.conf** under UNIX.
insert <*index number to insert at*> <*IP address of syslog server to add*> <*local facility number*> Assigns a specific index number to the syslog server you add. The index number you specify must be in use. Syslog servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*> Moves a syslog server up or down in the list of configured servers. The index numbers you specify must be in use. To view all syslog servers currently added to the system configuration, use the **list** command.

/cfg/sys/accesslist System Access Configuration

```
[Access List Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
```

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

Note:

If you are about to join one or more VPN Gateways to the cluster, the IP address of Interface 1 for all VPN Gateways in the cluster and the Management IP address (MIP) must be added to the Access list, before joining the new AVG. Otherwise the devices will not be able to communicate. This is however required only if the Access list consists of other entries, that is, IP addresses for control of Telnet and SSH access.

Table 234: Access List Menu Options (/cfg/sys/accesslist)

Command Syntax and Usage
list Displays all entries in the access list by index number, network address, and network mask.
del <*index number*> Removes an entry in the access list, specified by index number.
add <*host IP address*> <*subnet mask*> Adds a single machine, or a range of machines on a specific network, to the access list. Only those machines listed will be allowed to access the VPN Gateway through a Telnet or SSH connection (assuming that Telnet or SSH connections, or both, are enabled). To enable Telnet or SSH connections, see the **telnet** and **ssh** commands under /cfg/sys/adm Administrative Applications Configuration on page 427.

/cfg/sys/adm Administrative Applications Configuration

```
[Administrative Applications Menu]
snmp - SNMP menu
sonmp- Set SONMP Protocol participation
clitimeout - Set CLI idle timeout
audit- Audit Settings Menu
auth - Authentication menu
telnet     - Set telnet CLI access
ssh  - Set SSH CLI access
http - HTTP access menu
https- HTTPS access menu
sshkeys    - SSH host keys menu
enanumpool - Set Status of the IP Pool list
```

The Administrative Applications menu is for example used to manage access for different applications that can be used to administer the VPN Gateway software.

Table 235: Administrative Applications Menu Options (/cfg/sys/adm)

Command Syntax and Usage
snmp Displays the SNMP menu. To view menu options, see /cfg/sys/adm/snmp SNMP Management Configuration on page 429.
sonmp on|off Lets you enable SONMP (SynOptics Network Management Protocol) participation. SONMP is an Avaya-proprietary layer-2 protocol for discovering the topology of a network that contains SONMP-aware devices. • **on:** Enables SONMP participation. • **off:** Disables SONMP participation. To view the current network topology (requires that **sonmp** is set to **on**), use the **/info/sonmp** command. The default setting is off.
clitimeout *<timeout value in seconds [300-604800]>* Sets the time frame of user inactivity for the automatic logout from the CLI to occur. The default idle timeout value is 600 seconds (10 minutes), and the maximum value is 604800 seconds (7 days). Note that a changed time-out value does not take effect until the next login. To specify a value in minutes, hours or days, enter an integer directly followed by the letter **m, h,** or **d**, e.g. **2h30m**. If you enter an integer not followed by one of these letters, seconds is implied.

Command Syntax and Usage
If you have unapplied configuration changes when automatically logged out from the CLI, the unapplied configuration changes will be lost. Make sure to save your configuration changes regularly by using the global **apply** command.
audit
Displays the Audit settings menu. To view menu options, see /cfg/sys/adm/audit Audit Configuration on page 435.
auth
Displays the Authentication menu. To view menu options, see /cfg/sys/adm/auth Authentication Configuration on page 437.
telnet on|off
Enables or disables Telnet access. When set to **on** and not having added machine(s) to the access list, all Telnet connections are allowed. When set to **on** and having added machine(s) to the access list, only the specified machine(s) are allowed Telnet access. When set to **off**, all Telnet connections are rejected, including connections from machine(s) added to the access list. To view Access List menu options, see /cfg/sys/accesslist System Access Configuration on page 426. The default Telnet setting is **off**.
ssh on|off
Enables or disables SSH access. When set to **on** and not having added machine(s) to the access list, all SSH connections are allowed. When set to **on** and having added machine(s) to the access list, only the specified machine(s) are allowed SSH access. When set to **off**, all SSH connections are rejected, including connections from machine(s) added to the access list. To view Access List menu options, see /cfg/sys/accesslist System Access Configuration on page 426. The default SSH setting is **off**.
http
Displays the HTTP access menu. To view menu options, see /cfg/sys/adm/http Browser-Based Management Configuration on page 441.
https
Displays the HTTPS access menu. To view menu options, see /cfg/sys/adm/https Browser-Based Management Configuration with SSL on page 442.
sshkeys
Displays the SSH Host Keys menu. To view menu options, see /cfg/sys/adm/sshkeys SSH Host Keys Configuration on page 443.
enanumpool <on|off>

Command Syntax and Usage
Lets you to enable or disable the setting of the number of IP Pools more than the default.

/cfg/sys/adm/snmp SNMP Management Configuration

```
[SNMP Menu]
ena  - Enable SNMP
dis  - Disable SNMP
versions   - Set SNMP versions supported
snmpv2-mib - SNMPv2-MIB menu
community  - SNMP community menu
users- SNMP USM Users Menu
target     - Notification target menu
event- DISMAN-EVENT-MIB menu
```

The 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 Gateway s store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

Table 236: SNMP Menu Options (/cfg/sys/adm/snmp)

Command Syntax and Usage
ena Enables network management through SNMP.
dis Disables network management through SNMP.
versions <*comma separated list of desired versions*> Lets you specify the allowed SNMP version(s). The default value is that all (v1, v2c and v3) SNMP versions are supported.
snmpv2-mib Displays the SNMPv2-MIB menu. To view menu options, see /cfg/sys/adm/snmp/snmpv2-mib SNMPv2-MIB Configuration on page 430.
community Displays the SNMP Community menu. To view menu options, see /cfg/sys/adm/snmp/community SNMP Community Configuration on page 431.
users

Command Syntax and Usage
Displays the SNMP Users menu for managing SNMPv3 users. To view menu options, see /cfg/sys/adm/snmp/users <number> SNMPv3 Users Configuration on page 431. If you type the index number of a new user, a wizard will prompt you for the information available on the SNMP Users menu.
target
Displays the Notification Target menu. To view menu options, see /cfg/sys/adm/snmp/target <id> SNMP Notification Target Configuration on page 433.
event
Displays the Event menu. To view menu options, see /cfg/sys/adm/snmp/event SNMP Event Configuration on page 434.

/cfg/sys/adm/snmp/snmpv2-mib SNMPv2-MIB Configuration

```
[SNMPv2-MIB Menu]
sysContact - Set sysContact
snmpEnable - Set snmpEnableAuthenTraps
```

The SNMPv2-MIB menu is used for configuring parameters in the standard SNMPv2 Management Information Base (MIB) for the system.

The sysName and sysLocation parameters are set per host, under **/cfg/sys/host #**.

Table 237: SNMPv2-MIB Menu Options (/cfg/sys/adm/snmp/snmpv2-mib)

Command Syntax and Usage
sysContact Designates a contact person for the managed AVG cluster, together with information on how to contact this person.
snmpEnable disabled|enabled
Enables or disables generating authentication failure traps. The default value is disabled.

/cfg/sys/adm/snmp/community SNMP Community Configuration

```
[SNMP Community Menu]
read - Set Read Community String
write- Set Write Community String
trap - Set Trap Community String
```

The SNMP Community menu is used for configuring the community aspects of the SNMP monitoring.

Table 238: SNMP Community Menu Options (/cfg/sys/adm/snmp/community)

Command Syntax and Usage
read Specifies the monitor community name that grants read access to the Management Information Base (MIB). If no monitor community name is specified, read access is not granted. The default monitor community name is public .
write Specifies the control community name that grants read and write access to the Management Information Base (MIB). If no control community name is specified, neither write nor read access is granted.
trap Specifies the trap community name that accompanies trap messages sent to the SNMP manager. If no trap community name is specified, the sending of trap messages is disabled. The default trap community name is trap .

/cfg/sys/adm/snmp/users <number> SNMPv3 Users Configuration

```
[SNMP User 1 Menu]
name - Set user name
seclevel   - Set Security level
permission - Set Permission
authproto  - Set Authentication Protocol
authpasswd - Set Authentication Password
privproto  - Set Privacy Protocol
privpasswd - Set Encryption Password
del  - Remove SNMP User
```

The SNMP User menu is used for adding an SNMPv3 user to the configuration, based on the User-based Security Model (USM) for version 3 of SNMP.

For more information about USM, see RFC2274.

Table 239: SNMP User Menu Options (/cfg/sys/adm/snmp/users)

Command Syntax and Usage
name Sets the desired USM user name.
seclevel none|auth|priv
Sets the desired degree of SNMP USM security. • **none.** SNMP access is granted without authentication. • **auth.** Sets the SNMP user password to be verified before granting SNMP access. SNMP information is transmitted in plain text. Also set a password using the **authpassword** command below. • **priv.** Sets the SNMP user password to be verified before granting SNMP access and encrypts all SNMP information with the user's individual key. Also set a password and an encryption key using the **authpassword** and **privpassword** commands below. The default value is **priv**.
permission <*comma separated list of permissions*>
Lets you specify the USM user's permissions. • **get.** Authorizes the user to perform SNMP get requests, that is, the user is granted read access to the Management Information Base (MIB). • **set.** Authorizes the user to perform SNMP set requests, that is, the user is granted write access to the Management Information Base (MIB). The **set** permission automatically implicates the **get** permission, that is, if the user has write access he will have read access as well. • **trap.** Authorizes the user to receive trap event messages and alarm messages. Enter the desired permissions separated by comma, e.g. **get**,**trap**.
authproto
Sets the authentication protocol for SNMP transmissions. The default value is **md5**.
authpasswd <*password of at least 8 characters*>
Sets the password for authentication. This is required if the security level is set to **auth** or **priv**. See the **seclevel** command above. The password must be at least 8 characters long.

Command Syntax and Usage
privproto
Sets the privacy protocol for SNMP transmissions. The default value is **aes**.
privpasswd *<password of at least 8 characters>*
Sets the USM user's individual encryption key. This is required if the security level is set to **priv**. See the **seclevel** command above. The password must be at least 8 characters long.
del
Deletes the current SNMPv3 user from the configuration.

/cfg/sys/adm/snmp/target <id> SNMP Notification Target Configuration

```
[Notification Target 1 Menu]
ip   - Set target IP address
port - Set target port
version    - Set SNMP version
user - Set USM user name
del  - Remove Notification Target
```

The SNMP Notification Target menu is used for configuring the notification target aspects of SNMP monitoring.

Table 240: SNMP Notification Target Menu Options (/cfg/sys/adm/snmp/target)

Command Syntax and Usage
ip <*SNMP manager IP address*> Sets the IP address of the SNMP manager, to which trap messages are sent.
port <*TCP port [162]*>
Sets the TCP port used by the SNMP manager. The default value is port number 162.
version v1|v2c|v3
Specifies the SNMP version used by the SNMP manager. The default SNMP version is **v2c**.
user <*press TAB to view configured USM users*>

Command Syntax and Usage
If version 3 is selected (see the **version** command above), specify the desired USM user (see /cfg/sys/adm/snmp/users <number> SNMPv3 Users Configuration on page 431).
del
Removes the current SNMP manager from the configuration.

/cfg/sys/adm/snmp/event SNMP Event Configuration

```
[Event Menu]
addmonitor - Adds a monitor
delmonitor - Deletes a monitor
addevent   - Adds a notification event
delevent   - Deletes a notification event
list - list current monitors and events
```

The Event menu is used to create custom monitoring definitions for the objects in the DISMAN-EVENT-MIB. Start by defining a monitor for polling an object from the MIB, then configure a value to which the polled object's value should be compared. If a match is found, a corresponding event is generated. The event sends an SNMP notification with information about the monitor.

Table 241: Event Menu Options (/cfg/sys/adm/snmp/event)

Command Syntax and Usage
addmonitor
Enter **help addmonitor** for on-screen instructions.
delmonitor *<name of monitor>*
To delete a previously configured monitor, type the name of the monitor following the **delmonitor** command.
addevent
Enter **help addevent** for on-screen instructions.
delevent
To delete a previously configured event, type the name of the event following the **delevent** command.
list
Lists all configured monitors and events once additions or changes have been applied.

/cfg/sys/adm/audit Audit Configuration

```
[Audit Menu]
servers    - RADIUS Servers Menu
vendorid   - Set vendor id for audit attribute
vendortype - Set vendor type for audit attribute
ena  - Enable Audit
dis  - Disable Audit
```

The Audit menu is used for configuring a RADIUS server to receive log messages about commands executed in the CLI or the BBI (Browser-Based Management Interface). If auditing is enabled but no RADIUS server is configured, events will still be generated to the event log and any configured syslog servers.

An event is generated whenever a user logs in/logs out or issues a command from a CLI session. The event contains information about user name and session id as well as the name of executed commands. This event is optionally sent to a RADIUS server for audit trail logging according to RFC 2866 (RADIUS Accounting).

For instructions on how to configure a RADIUS accounting server for logging Portal user sessions, see /cfg/vpn <id> /aaa/radacct RADIUS Accounting Configuration on page 246.

Table 242: Audit Menu Options (/cfg/sys/adm/audit)

Command Syntax and Usage
servers Displays the RADIUS Audit Servers menu. To view menu options, see /cfg/sys/adm/audit/servers RADIUS Audit Server Configuration on page 436.
vendorid Assigns the SMI Network Management Private Enterprise Code—as defined by IANA in the file http://www.iana.com/—to the Vendor-Id attribute. The Vendor-Id—represented by the private enterprise number—is a value for RADIUS' standard attribute `vendor-specific` (26). The default vendor-Id is set to **1872** (Alteon). **Note:** If another vendor-Id is used by your RADIUS system, you can use the **vendorid** command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. If you want to use a standard attribute type as defined in RFC 2865, set **vendorid** to **0**. Then configure the desired standard attribute type as the vendor type value.

Command Syntax and Usage
vendortype
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 audit attribute which will contain the audit information. The default vendor type value is set to 2. Tip! Finding audit entries in the RADIUS server's log can be made easier by defining a suitable string in the RADIUS server's dictionary (for example Alteon-SSL-Audit-Trail) and mapping this string to the vendor type value. **Note:** If another number for vendor type is used by your RADIUS system, you can use the **vendortype** command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. If you want to use a standard attribute type as defined in RFC 2865, set **vendorid** to **0**. Then configure the desired standard attribute type as the vendor type value.
ena
Enables auditing, which means that CLI or BBI login, logout and update events are sent to the event log, any configured syslog servers and to a RADIUS audit server. The RADIUS server must however be configured on the VPN Gateway (see /cfg/sys/adm/audit/servers RADIUS Audit Server Configuration on page 436).
dis
Disables auditing, which means that no audit events will be generated.

/cfg/sys/adm/audit/servers RADIUS Audit Server Configuration

```
[RADIUS Audit Servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The RADIUS Audit servers menu is used for adding, modifying and deleting information about RADIUS audit servers.

Table 243: RADIUS Audit Servers Menu Options (/cfg/sys/adm/audit/servers)

Command Syntax and Usage
list Lists the IP addresses of currently configured RADIUS audit servers, along with their corresponding index numbers.
del Removes the specified RADIUS audit server from the configuration. Use the **list** command to display the index numbers of all added RADIUS audit servers.
add <*IP address*> <*TCP port number*> <*shared secret*> Adds a RADIUS audit server to the configuration. Specify the IP address, a TCP port number, and the shared secret. The next available index number is assigned automatically by the system. For backup purposes, several RADIUS audit servers can be added. The VPN Gateway will contact the server with lowest index number first. If contact could not be established, the AVG will try to contact the server with the next index number in sequence and so on. **Note:** The default port number used for RADIUS audit is 1813.
insert <*index number to insert at*> <*IP address of RADIUS audit server to add*> Assigns a specific index number to the RADIUS audit server you add. The index number you specify must be in use. RADIUS audit servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*> Moves a RADIUS audit server up or down in the list of configured servers. The index numbers you specify must be in use. To view all servers currently added to the configuration, use the **list** command.

/cfg/sys/adm/auth Authentication Configuration

```
[Authentication Menu]
servers    - RADIUS Authentication Servers menu
timeout    - Set RADIUS server timeout
fallback   - Use local password as fallback
group- RADIUS Group Attribute menu
ena  - Enable RADIUS Authentication
dis  - Disable RADIUS Authentication
```

The Authentication menu is used to configure RADIUS authentication of system users. Authentication applies to both CLI and BBI (Browser-Based Management Interface) users.

Note:

When RADIUS authentication of system users is enabled, it applies also to CLI access through the console, and to the "root" login. The "boot" login used for software reinstall will however always use the fixed local password.

Table 244: Authentication Menu Options (/cfg/sys/adm/auth)

Command Syntax and Usage
servers Displays the RADIUS Authentication Servers menu. To view menu options, see /cfg/sys/adm/auth/servers Authentication Servers Configuration on page 439.
timeout <*value in seconds*> Sets a timeout value in seconds for a connection request to a RADIUS server. If the timeout value elapses before a connection is established, authentication will fail. The default RADIUS server timeout value is 10 seconds.
fallback on|off Sets the desired fallback mode. • **on:** The local passwords (for example the admin password) are used as fallback if the RADIUS servers are unreachable. Note that unwanted access to a VPN Gateway through serial cable will be possible if the network cable is disconnected and the local password is known. • **off:** If the RADIUS servers are unreachable, the only way to access the system is to reinstall the software (boot install). The default value is **on**.
group Displays the RADIUS Group Attribute menu. To view menu options, see /cfg/sys/adm/auth/group RADIUS Group Attribute Configuration on page 440.
ena Enables RADIUS authentication of system users (disabled by default).
dis Disables RADIUS authentication of system users (disabled by default).

/cfg/sys/adm/auth/servers Authentication Servers Configuration

```
[RADIUS Authentication Servers Menu]
list - List all values
del  - Delete a value by number
add  - Add a new value
insert     - Insert a new value
move - Move a value by number
```

The RADIUS Authentication Servers menu lets you add one or more RADIUS authentication servers to the configuration.

Table 245: RADIUS Authentication Servers Menu Options (/cfg/sys/adm/auth/servers)

Command Syntax and Usage
list Lists the IP addresses of currently configured RADIUS authentication servers, along with their corresponding index numbers.
del Removes the specified RADIUS authentication server from the configuration. Use the **list** command to display the index numbers of all added RADIUS authentication servers.
add <*IP address*> <*TCP port number*> <*shared secret*> Adds a RADIUS authentication server to the configuration. Specify the IP address, a TCP port number, and the shared secret. The next available index number is assigned automatically by the system. For backup purposes, several RADIUS servers can be added. The VPN Gateway will contact the server with lowest index number first. If contact could not be established, the AVG will try to contact the server with the next index number in sequence and so on. **Note:** The default port number used for RADIUS authentication is 1812.
insert <*index number to insert at*> <*IP address of RADIUS authentication server to add*> Assigns a specific index number to the RADIUS authentication server you add. The index number you specify must be in use. RADIUS authentication servers with an index number higher than (and including) the one you specify will have their current index number incremented by 1.
move <*index number to move*> <*destination index number*>

Command Syntax and Usage
Moves a RADIUS authentication server up or down in the list of configured servers. The index numbers you specify must be in use. To view all servers currently added to the configuration, use the **list** command.

/cfg/sys/adm/auth/group RADIUS Group Attribute Configuration

```
[RADIUS Group Attribute Menu]
vendorid   - Set vendor id for group attribute
vendortype - Set vendor type for group attribute
ena  - Enable group attribute usage
dis  - Disable group attribute usage
```

The RADIUS Group Attribute menu lets you configure the VPN Gateway to authorize administrator users based on a group attribute sent by the RADIUS authentication server. When the user is successfully authenticated, the RADIUS server returns the groups to which the user belongs. The groups are compared to the fixed administrator groups on the VPN Gateway, that is, tunnelguard, admin, oper and certadmin. If a match is found, the logged on user is given the administration rights pertaining to matching group(s). Otherwise, the user is denied access.

The RADIUS system administrator can thus add VPN Gateway administrator users to the RADIUS configuration without being an administrator of the AVG, because the users do not need to be configured locally on the AVG. By assigning suitable administrator groups to these users, the users can be given the desired access rights to the CLI/BBI.

Table 246: RADIUS Group Attribute Menu Options (/cfg/sys/adm/auth/group)

Command Syntax and Usage
vendorid <*integer value*> Assigns the SMI Network Management Private Enterprise Code – as defined by IANA in the filehttp://www.iana.org/ – to the Vendor-Id attribute. The default Vendor-Id is 1872 (Alteon). **Note:** If another Vendor-Id is used by your RADIUS system, you can use the **vendorid** command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. **Note:** If you want to use a standard attribute type (as defined in RFC 2865) set **vendorid** to 0. Then configure the desired standard attribute type as the

Command Syntax and Usage
vendor type value (see next command). For example, to use the standard attribute Class, set **vendorid** to 0 and vendor **type** to 25.
vendortype <*integer value*>
Assigns a number to the Vendor-Type attribute used in RADIUS. Used in combination with the Vendor-Id, the Vendor-Type number identifies the group in which users who should be allowed access to the CLI/BBI through RADIUS authentication are members. The default Vendor-Type value is 1. The usage of the Vendor-Type attribute conforms to the recommendations in RFC 2865, section 5.26. **Note:** If another number for vendor type is used by your RADIUS system, you can use the **vendortype** command to bring the RADIUS configuration in line with the value used by the remote RADIUS system. Contact your RADIUS system administrator for more information. **Note:** If **vendorid** is set to 0, **vendortype** should be set to a standard attribute type as defined in RFC 2865. For example, to use the standard attribute Class, set **vendorid** to 0 and **vendortype** to 25.
ena
Enables usage of group attributes (disabled by default).
dis
Disables usage group attributes (disabled by default).

/cfg/sys/adm/http Browser-Based Management Configuration

```
[HTTP Menu]
port - Set HTTP Server port
ena  - Enable server
dis  - Disable server
```

The HTTP menu is used for enabling/disabling browser-based configuration of your VPN Gateway. To access the Browser-Based Management Interface (BBI), enter the Management IP address assigned to your AVG cluster in your web browser.

Table 247: HTTP Menu Options (/cfg/sys/adm/http)

Command Syntax and Usage
port

Command Syntax and Usage	
	Sets the port number to be used for browser-based AVG configuration using the BBI. The default port number is 80.
ena	
	Enables the HTTP server used for browser-based configuration on the VPN Gateway.
dis	
	Disables the HTTP server used for browser-based configuration on the VPN Gateway.

/cfg/sys/adm/https Browser-Based Management Configuration with SSL

```
[HTTPS Menu]
port - Set HTTPS Server port
cert - Set server certificate
ena  - Enable server
dis  - Disable server
```

The HTTPS menu is used for enabling/disabling browser-based configuration of your VPN Gateway through a secure SSL tunnel. To access the Browser-Based Management Interface (BBI), enter the Management IP address assigned to your AVG cluster in your web browser.

Table 248: HTTPS Menu Options (/cfg/sys/adm/https)

Command Syntax and Usage	
port	
	Sets the port number to be used for browser-based AVG configuration from the BBI using SSL. The default port number is 443.
port	
	Sets the port number to be used for browser-based AVG configuration from the BBI using SSL. The default port number is 443.
ena	
	Enables the HTTPS server used for browser-based configuration on the VPN Gateway using SSL.

Command Syntax and Usage
dis
Disables the HTTPS server used for browser-based configuration on the VPN Gateway using SSL.

/cfg/sys/adm/sshkeys SSH Host Keys Configuration

```
[SSH Host Keys Menu]
generate   - Generate new SSH host keys for the cluster
show - Show current SSH host keys for the cluster
knownhosts - SSH known host keys menu
```

The SSH Host Keys menu is used to generate new SSH host keys for the cluster. It also lets you display the current host keys in the CLI. To manage known host keys, proceed to the SSH Known Host Keys menu.

For more information about SSH Host Keys and their usage, see Appendix G, "SSH Host Keys", in the *User's Guide*.

Table 249: SSH Host Keys Menu Options (/cfg/sys/adm/sshkeys)

Command Syntax and Usage
generate
Generates new SSH host keys (RSA1, RSA and DSA). The keys are used by all hosts in the cluster in accordance with the Single System Image (SSI) concept, that is, connections to the management IP address (MIP) will always appear to a SSH client to be to the same host. After having generated new SSH host keys, activate the new keys by using the **apply** command.
show
Shows the current SSH host keys for the cluster. The keys and corresponding fingerprints are displayed directly in the CLI. There is no standard format for RSA1 keys – the format used in the CLI output is that of the OpenSSH implementation, except that the single line of this format is wrapped. It may need to be edited back into a single line for use in the key storage of an SSH client. For RSA and DSA keys, the "SECSH Public Key File Format" per Internet Draft draft-ietf-secsh-publickeyfile is used.
knownhosts
Displays the SSH known host keys menu. To view menu options, see /cfg/sys/adm/sshkeys/knownhosts SSH Known Host Keys Configuration on page 444.

/cfg/sys/adm/sshkeys/knownhosts SSH Known Host Keys Configuration

```
[SSH Known Host Keys Menu]
list - List known SSH keys of remote hosts
del  - Delete known SSH host key by index
add  - Add a new SSH host key
import     - Retrieve SSH key from remote host
```

The SSH Known Host Keys menu is used to manage known host keys, for example paste or import SSH keys from known remote hosts.

For more information about known host keys and their usage, see Appendix G, "SSH Host Keys", in the *User's Guide*.

Table 250: SSH Known Host Keys Menu Options (/cfg/sys/adm/sshkeys/knownhosts)

Command Syntax and Usage
list Lists the type and fingerprint of the known SSH keys for remote hosts.
del Deletes the desired known SSH host key by index number.
add Lets you paste a new SSH host key. The format can be either that of the **/cfg/sys/adm/sshkeys/show** command, or the native format used by the OpenSSH implementation. If the key has a valid format, you will be prompted for the corresponding host name or IP address - it is also possible to give a comma-separated list of names and/or IP addresses for the host.
import <*IP address of remote host*> Lets you import an SSH key from a remote host. This is mainly a convenience function, to avoid the prompt to accept a new key at a later use of SCP or SFTP for file or data transfer. In particular, the security implications are exactly the same, and to achieve strict "man in the middle" protection, the fingerprint should be verified before applying the changes.

/cfg/sys/user User Access Configuration

```
[User Menu]
passwd     - Change own password
expire     - Set password expire time interval
list - List all users
del  - Delete a user
add  - Add a new user
edit - Edit a user
caphrase   - Certadmin export passphrase
```

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.

The password for the boot user cannot be changed. The reason for this is that if you would lose both the admin password and the boot password, the default passwords could not be restored even by performing a reinstallation of the software (only the boot user can do this). For more information about default user accounts and related access levels, see the "Accessing the AVG "section in the "Command Line Interface" chapter in the *User's Guide*.

Table 251: User Menu Options (/cfg/sys/user)

Command Syntax and Usage
passwd *<own login password> <new password> <confirm new password>* Lets you change your current login password. The password can contain spaces and is case sensitive.
expire *<time in days, e.g. 10d for 10 days>* Sets an expiration time for system operator passwords. The time applies to all system users. The counter starts at the time when the new expiration time is set. The first time the operator logs on after the specified time has expired, he or she is prompted for a new password. The default expiration time is 0, that is, no expiration time.
list Lists all user accounts. The three built-in users are always listed: admin , oper , and root .
del *<username>* Removes the specified user account from the system. Of the three built-in users (admin , oper , and root) only the oper user can be deleted. Only users with Administrator rights can delete user accounts.

Command Syntax and Usage
add <*username*>
Adds a user account to the system. After having added a user account, you must also assign the user account to a group. See the **groups** command on groups groupsfor more information. Only users with Administrator rights can add user accounts.
edit <*username*>
Displays the User <*username*> menu. To view menu options, see /cfg/sys/user/edit <username> Edit User Menu on page 446.
caphrase <*cert admin export passphrase*> <*confirm cert admin export passphrase*>
Sets the certificate administrator's passphrase for encrypted private keys in a configuration backup. As long as the admin user is a member of the certadmin group (the default setting), the admin user is prompted for an export passphrase to protect the private keys in the configuration dump each time the **/cfg/ptcfg** command is used. A certificate administrator export passphrase need only be defined if the admin user has removed himself or herself from the certadmin group, and added a certificate administrator user with certadmin group rights. The certadmin export passphrase will then automatically be used (without prompting the user) to protect the encrypted private keys in the configuration backup when the **/cfg/ptcfg** command is performed. Upon restoring a configuration backup from a TFTP/FTP/SCP/SFTP server (**/cfg/gtcfg**), the user will be prompted for the correct certadmin passphrase as defined using the **caphrase** command. **Note:** The **caphrase** menu command is only displayed when the logged in user is a member of the **certadmin** group.

/cfg/sys/user/edit <username> Edit User Menu

```
 [User  <username>   Menu]
          password     -Login password
groups      -  Groups menu
cur           - Display current setting
```

The User <*username*> menu is used to set or change the login password for a specified user. Only users with Administrator rights can perform this tasks, and then only if the admin user is a member of the same group as the other user. The **groups** menu option gives access to the Groups menu, in which the group assignment for the specified users is set.

Table 252: User <username> Menu Options (/cfg/sys/user/edit)

Command Syntax and Usage
password *<own login password> <login password for user> <confirm login password for user>* Sets the login password for the specified user. The password can contain spaces and is case sensitive.
groups Displays the Groups menu. To view menu options, see /cfg/sys/user/edit <username> /groups User Access Groups Menu on page 447.
cur Displays the current group settings for the specified user.

/cfg/sys/user/edit <username> /groups User Access Groups Menu

```
[Groups Menu]
list - List all values
del  - Delete a value by number
add        - Add a new value
```

The Groups menu is used to set or change the group assignment for a user. Whenever a new user account is added, the new user must be assigned to a group. Only the Administrator user can add a new user account to the system, but any user can grant an existing user membership in a group in which the granting user is already a member.

By default, the Administrator user is a member of all four built-in groups and can therefore add a new user to any of these groups. A certificate administrator however, which presumably is a member of the certadmin group, can only add an existing user to the certadmin group.

Table 253: Groups Menu Options (/cfg/sys/user/edit/groups)

Command Syntax and Usage
list Lists the current group assignment of the specified user.
del *<group by index number>* Removes the user from the specified group. Only users with Administrator rights can remove other users from groups.
add *<group name* **[admin|oper|tunnelguard|certadmin]** >

Command Syntax and Usage
Assigns the specified user to one of the built-in groups: admin , oper , tunnelguard or certadmin . To assign yet another group to the current user, use the **add** command once again.

/cfg/sys/cur Current System Configuration

```
 System:
Management IP (MIP) address = 10.1.82.144
Cluster Host 1:
Type of the host = master
IP address = 10.1.82.145
SysName =
SysLocation =
License =
IPSEC user sessions: 250
Secure Service Partitioning
PortalGuard
TPS: unlimited
SSL user sessions: 250
Default gateway address = 10.1.82.2
Ports = 1 : 2
Hardware platform = 3070
Host Routes:
No items configured
Host Interface 1:
IP address = 10.1.82.145
Network mask = 255.255.255.0
VLAN tag id = 0
Mode = failover
Primary port = 0
Host Interface Routes:
No items configured
Interface Ports:
2
Host Port 1:
Autonegotiation = on
Speed = 0
Full or half duplex mode = full
Host Port 2:
Autonegotiation = on
Speed = 0
Full or half duplex mode = full
Routes:
No items configured
```

/cfg/lang Language Support Configuration

```
[Language Support Menu]
import     - Import language definition file
export     - Export language definition template
list - List the loaded languages
vlist- List ISO 639 language codes
del  - Delete (custom) language definition
```

The Language Support menu is used for managing language definition files. A language definition file is used for Portal localization, that is, the ability to customize the language displayed on buttons, tabs, prompts and similar on the Portal pages.

Table 254: Language Support Menu Options (/cfg/lang)

Command Syntax and Usage
import <*protocol* **[tftp|ftp|scp|sftp]**> <*server by host name or IP address*> <*name of language definition file*> <*ISO 639 language code*>
Imports a ready-to-use language definition file from the specified TFTP/FTP/SCP/SFTP file server. As you import the file, you are prompted for an ISO 639 language code. To view valid language codes, use the **vlist** command. The language code is saved to the configuration together with the imported language definition file. To set the desired language for the Portal of a specific VPN, select the language code using the **/cfg/vpn <id>/portal/lang** command.
export <*protocol* **[tftp|ftp|scp|sftp]**> <*server by host name or IP address*> <*name of template file*> <*ISO 639 language code*>
Exports the language definition template (or loaded language definition file if any) to the specified TFTP/FTP/SCP/SFTP file server. Once exported, screen text (for example button and field labels) can be translated to the desired language directly in the file. When translation is done, the file can be uploaded to a TFTP/FTP/SCP/SFTP server for import to the VPN Gateway using the **import** command (see above).
list
Lists the languages that are added to the configuration by language code and description. English (en) is the predefined language and is always present.
vlist
Lists all valid languages codes and the corresponding language description. To list all valid language codes beginning with a specific letter, enter the **vlist** command followed by the desired letter. Example: Enter **vlist c** to display all language codes beginning with the letter c .

Command Syntax and Usage
del *<language code, e.g. sve for Swedish>*
By entering this command followed by a language code, the corresponding language definition file will be deleted from the configuration. You cannot delete a language file that is currently in use. English (en) is the predefined language and cannot be deleted.

/cfg/bwm Bandwidth Management

```
[Bandwidth Management Menu]
      ena         - Enable Bandwidth Management
      dis         - Disable Bandwidth Management
      bwmpolicy   - Bandwidth management policy menu
      info        - Print the bandwidth management info
      ipsecpass   - IPsec passthrough menu
```

Bandwidth Management 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.

Note:

Up to 255 bandwidth management contracts can be configured.

Table 255: Bandwidth Management menu options (cfg/bwm)

Command Syntax and Usage
ena Enables Bandwidth Management.
dis Disables Bandwidth Management.
bwmpolicy <bwm policy name/number (1-255)> <policy name> <hard limit (2000-400000)> <soft limit (2000-400000)> Displays the Bandwidth Policy Management Menu. To view menu options, see /cfg/bwm/bwmpolicy Bandwidth Management Policy on page 451. Enter the following details to view Bandwidth Management Policy Menu:

Command Syntax and Usage
• `Enter bwm policy number or name` : defines the policy number for the contract. It value ranges from 1 to 255. • `Enter the soft limit` : sets the soft bandwidth limit for this policy. The value ranges from 2000 to 400000. • `Enter the hard limit` : sets the hard bandwidth limit for this policy. This is the highest amount of bandwidth available to this policy. The value ranges from 2000 to 400000.
info
Displays the Bandwidth Management information.
ipsecpass
Displays the IPsec Passthrough Menu. For more information about options, see /cfg/bwm/ipsecpass IPsec Passthrough on page 452.

/cfg/bwm/bwmpolicy Bandwidth Management Policy

```
[Bandwidth Management Policy 1 Menu]
      name       - Set policy name
      soft       - Set soft limit
      hard       - Set hard limit
      comment    - Set comment
      del        - Bandwidth Management Prolicy
```

Use the Bandwidth Management Policy Menu to configure a single BWM policy for multiple groups and extended profiles.

Table 256: Bandwidth Management Policy Menu options (cfg/bwm/bwmpolicy)

Command Syntax and Usage
name <policy name> Displays the policy name and lets you change it.
soft <2000 to 400000>
The soft limit is the desired or minimum guaranteed rate for a bandwidth policy. When the output bandwidth is available, a bandwidth class is allowed to send data at this rate. The soft limit ranges from 2000 to 400000 kilobits and the default value is 2000 kilobits.
hard <2000 to 400000>
Displays the hard limit value and lets you change it. The hard limit is the upper boundary for the policy. A bandwidth class is never allowed to transmit above the hard limit. The hard limit ranges from 2000 to 400000 kilobits and the default value is 2000 kilobits.

Command Syntax and Usage
comment
Displays the comment for the BWM policy and lets you change it.
del
Deletes the BWM policy.

/cfg/bwm/ipsecpass IPsec Passthrough

```
[IPsec Passthrough Menu]
      ena         - Enable IPsec passthrough
      dis         - Disable IPsec passthrough
      servers     - IPsec servers menu
      bwpolicy    - Set BW Policy
```

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.

Table 257: IPsec Passthrough menu options (cfg/bwm/ipsecpass)

Command Syntax and Usage
ena
Enables IPsec pass through.
dis
Disables IPsec pass through.
servers
Displays IPsec Servers menu. To view menu options, see /cfg/bwm/ipsecpass/servers IPsec Servers on page 453.
bwpolicy
Displays the BWM policy name and lets you to change it.

/cfg/bwm/ipsecpass/servers IPsec Servers

```
[IPsec servers menu Menu]
      list       - List all values
      del        - Delete a value by number
      add        - Add a new value
      insert     - Insert a new value
      move       - Move a value by number
```

Table 258: IPsec Servers menu options (cfg/bwm/ipsecpass/servers)

Command Syntax and Usage
lists Displays all the configured values.
del <index number> Deletes the value from the index number.
add <IP address> Adds the IP address.
move <index number to move> <destination index> Moves the value from the current index number to the destination index.

/cfg/log Logging system configuration

```
[Logging System Menu]

in-memory            - Log in memory
```

Logging information can be cached in internal buffer. The Network devices collects and accesses this information.

/cfg/log/ in-memoryInternal memory configuration

```
[Internal Memory Menu]

onoff       - Set to Enable or Disable Internal Memory.
```

```
buffersize   - Set to configure the size of the internal buffer.

displaycfg   - To display the current configuration Settings.
```

All the log messages will be stored in the internal memory.

Table 259: Citrix menu (/cfg/log/in-memory)

Command Syntax Usage
onoff When set to on, internal memory is enabled. Default value is off.
buffersize Sets the size of the internal buffer. You can enter the buffersize ranging from 200 to 500.
displaycfg Displays the following configuration settings: • the internal memory status whether it is set to on or off. • the internal memory log status. • maximum message in the memory (which is 300).

/boot Boot Menu

The Boot menu is used for managing software versions, and to shutdown, reboot, or reset the configuration of a particular VPN Gateway. To use the Boot menu, you must be logged in as the Administrator user.

```
[Boot Menu]
software   - Software management menu
halt- Halt the iSD
reboot     - Reboot the iSD
delete      - Delete the iSD
```

During normal operations, when you are connected through Telnet or SSH to the Management IP (MIP) address, all VPN Gateways in the cluster are up, and cluster communications are working as expected, you can halt, reboot, or delete a VPN Gateway using the commands in the iSD Host menu. For more information on iSD Host menu options, see /cfg/sys/host <id> iSD Host Configuration on page 410.

If the VPN Gateway you want to halt, reboot, or delete has become isolated from the cluster, you can connect to that particular VPN Gateway either through Telnet or SSH (using the AVG 's individually assigned IP address), or use a console connection to perform the **halt**,

reboot, or **delete** commands from the Boot menu instead. To view the operational status of each VPN Gateway in the cluster, use the command **/info/isdlist**.

Table 260: Boot Menu Options (/boot)

Command Syntax and Usage
software Displays the Software Management menu. To view menu options, see /boot/software Software Management Menu on page 456.
halt Stops the particular VPN Gateway to which you have connected through Telnet, SSH, or a console connection. Always use this command before turning off the device. If you are connected through Telnet or SSH to the Management IP address (MIP), use the **halt** command in the iSD Host menu (**/cfg/sys/host #**) instead.
reboot Reboots the particular VPN Gateway to which you have connected through Telnet, SSH or a console connection. If you are connected through Telnet or SSH to the Management IP address (MIP), use the **reboot** command in the iSD Host menu (**/cfg/sys/host #**) instead.
delete Resets the particular VPN Gateway to which you have connected through Telnet, SSH, or a console connection, to its factory default configuration (all IP configuration is lost). The software itself will remain intact. After having performed a **delete** , you can only access the device through a console connection. Log in as the admin user with the admin password to enter the Setup menu. **Note:** If you receive a warning saying that the VPN Gateway you are trying to delete has no contact with any (other) master VPN Gateway in the cluster, you should also connect to the MIP address through Telnet or SSH and delete the VPN Gateway from the cluster by using the **delete** command in the iSD Host menu (**/cfg/sys/host #**). The **/boot/delete** command is primarily intended for situations when you want to delete a VPN Gateway that has either become isolated from the cluster, or has been physically removed from the cluster without first performing the **delete** command from the iSD Host menu (for more information about the iSD Host menu options, see /cfg/sys/host <id> iSD Host Configuration on page 410). In these situations, you must use the **/boot/delete** command to present the Setup menu, from which you can perform the **new** and **join** commands.

Command Syntax and Usage
Note: When using the **/boot/delete** command on the ASA 310 FIPS model, you also have the option to reset the HSM cards on the particular ASA 310 FIPS to which you have connected. For detailed information about resetting the HSM cards, see the "Resetting.HSM Cards on the ASA 310-FIPS" section in the "Troubleshooting the" chapter in the *User's Guide*.

/boot/software Software Management Menu

```
[Software Management Menu]
cur  - Display current software status
activate   - Select software version to run
download   - Download a new software package through FTP/SCP/SFTP
del  - Remove unpacked/old releases
```

The Software Management menu is used to show the current software status of the particular VPN Gateway to which you have connected. The menu is also used to download software upgrade packages through TFTP/FTP/SCP/SFTP, as well as activating or deleting a software upgrade package.

Table 261: Software Management Menu Options (/boot/software)

Command Syntax and Usage
cur Displays the software status of the particular VPN Gateway to which you have connected through Telnet, SSH, or a console connection. For a sample screen output, see /boot/software/cur Current Software Status Command on page 457.
activate <*software version as listed when using the* **cur** *command*> Activates a downloaded software upgrade package indicated as unpacked (when using the **cur** command). If serious problems occur while running the new software version, you may switch back to the previous version by activating the software version indicated as old (when using the **cur** command). Note that you will be logged out upon confirming the **activate** command.
download <*protocol* [ftp|scp|sftp]> <*server host name or IP address*> <*filename*> <*FTP server user name and password*> Downloads a new software package from a FTP/SCP/SFTP server, to perform a minor or major upgrade. You need to provide the host name or IP address of the server, as well as the file name of the software upgrade package. Software upgrade packages typically have the **.pkg** file name extension.

Command Syntax and Usage
If you include a directory path and file name (separated by a forward slash (/)) on the same line as the FTP server host name or IP address when you run the command, make sure you put the combined directory path and file name string within double quotation marks. Example: `>> Software Management#` **`download ftp 10.0.0.1 "pub/SSL-7.0.1-upgrade_complete.pkg"`** If you are using anonymous mode when downloading the software package from an FTP server, the following string is used as the password (for logging purposes): **`admin@'hostname'.isd`**
`del`
Removes a software upgrade package that has been downloaded, in case you do not want to activate the unpacked software upgrade package. Only software versions whose status is indicated as unpacked (using the **`cur`** command) can be removed.

/boot/software/cur Current Software Status Command

```
  >> Software Management#  cur
  Version                    Name                    Status
-------                    ----                    ------
7.0.1                       SSL                    permanent
5.1.5                       SSL                     old
```

This command displays information about the software version that is currently operational (`permanent`), and the software version that preceded the currently operational software version (`old`). If you have downloaded a software upgrade package and not yet activated it, the software upgrade package is indicated as `unpacked` . After activating a software version indicated as either `unpacked` or `old` , that version's status is propagated to `permanent` (after the VPN Gateway has performed a reboot).

/maint Maintenance Menu

The commands in the Maintenance menu are used to send log file information, or information about the current system internal status, collected from one or all VPN Gateways, to a TFTP or FTP server for technical support purposes.

```
[Maintenance Menu]
```

```
hsm             - HSM menu

log             - Logging system

tsdmp           - Dump local info, node status, configuration etc

dumplogs        - Tech support dump log files to TFTP/FTP/SFTP server

dumpstat        - Tech support dump current status to TFTP/FTP/SFTP server

chkcfg          - Check applied configuration

starttrace      - Start Trace

stoptrace       - Stop Trace
```

Note:

The HSM menu is only accessible for ASA 310-FIPS devices.

Table 262: Maintenance Menu Options (/maint)

Command Syntax and Usage
hsm Displays the HSM menu. To view menu options, see /maint/hsm Hardware Security Module Menu on page 460.
dumplogs *<protocol* [tftp|ftp|sftp]> *<server host name or IP address> <destination file name> <collect info from all iSDs?> <FTP user name and password>*
Collects system log file information from the VPN Gateway you are connected to (or optionally, all AVGs in the cluster) and sends the information to a file in the gzip compressed tar format on the TFTP or FTP server you have specified. The information can then be used for technical support purposes. The file sent to the TFTP/FTP/SFTP server does not contain any sensitive information related to the system configuration, such as certificates, private keys, and so on.
log
A logging system is used to cache the logging information in the internal buffer. This allows network to collect and access the logging information.
tsdmp
Creates a dump of the local information, status of nodes, statistics, events and alarms, and configuration in one place.

Command Syntax and Usage
dumpstat <*protocol* **[tftp|ftp|sftp]**> <*server host name or IP address*> <*destination file name*> <*collect info from all iSDs?*> <*FTP user name and password*>
Collects current system internal status from the VPN Gateway you are connected to (or optionally, all AVGs in the cluster) and sends the information to a file in the gzip compressed tar format on the TFTP/FTP/SFTP server you have specified. The information can then be used for technical support purposes.
chkcfg

Checks if the VPN Gateway is able to contact configured gateways, routes, DNS servers and authentication servers. The command also checks if the VPN Gateway can connect to web servers specified in group links. Besides checking the connection, the method (for example ping) for checking each item is displayed. Below is an example of the CLI output after having executed the **chkcfg** command:
`Checking configuration from 192.168.128.210`
`Testing /cfg/sys/host 1/gateway:192.168.128.3... ping ok`
`Testing /cfg/sys/dns/servers:192.168.128.1... dns ok`
`Testing /cfg/vpn 1/aaa/group 1/link 1:www.cnn.com:80... tcp ok`
`All tests completed successfully`

starttrace
Logs information pertaining to a VPN user session, for example SSL handshake specifics, authentication method, DNS lookups, user name, group, profile and so on. The trace feature can be used as a debugging tool, for example to find out why authentication fails. For sample outputs, see the "Troubleshooting the" chapter in the *User's Guide*. • Enter tag. To limit tracing to specific features or subsystems, enter the desired tag or a comma separated list of tags, e.g. aaa or aaa,dns. To trace all features, press ENTER. - aaa: Logs authentication method, user name, group, timeouts and profile (base or extended). - dns: Logs failed DNS lookups made during a VPN session. - ike: Logs any output that is produced by the IKE daemon, for example all messages related to actual ISAKMP negotiations between the client and the IKE daemon. - ipsec: Logs any AAA-related output concerning the establishment of an IPsec tunnel. - ippool: Logs messages related to the allocation of IP addresses from the IP pools (applies to Net Direct and IPsec). - ssl: Logs information related to the SSL handshake procedure, for example used cipher. - tg: Logs information related to a Tunnel Guard check, for example access method, user name, user source IP, Tunnel Guard session status and SRS rule check result.

Command Syntax and Usage
- upref: Shows retrieval and storage of user preferences (if any), for example Portal bookmarks. - smb: Logs information related to Portal SMB (Windows file share) sessions. - ftp: Logs information related to Portal FTP sessions. - netdirect: Logs information pertaining to the Net Direct client connection, for example that a connection has been requested and that it has been accepted or rejected. - netdirect_packet: Logs information about packets being sent and received when the user has initiated a connection to a host. - SPO: Logs information pertaining to the SPO client connection. • Enter VPN. To limit tracing to a specific VPN, enter the desired VPN ID. To use tracing for all VPNs, press ENTER or enter 0 as VPN ID. • Output mode. If set to **interactive** , the information will be logged directly in the CLI when a user authenticates to the Portal. By selecting **tftp**, **ftp** or **sftp**, the output can instead be logged to an TFTP/FTP/SFTP server.
stoptrace Stops tracing. If **interactive** output mode is selected and information has been logged to the CLI, press ENTER to redisplay the CLI prompt.

/maint/hsm Hardware Security Module Menu

```
[HSM Menu]
login- Login to HSM cards on local iSD
splitkey   - Split a wrap key onto CODE iKeys
changepass - Change iKey password
```

The HSM menu is used for logging in to the HSM card on a local ASA 310-FIPS device after a reboot has occurred. It is also used for splitting the wrap key onto a set of HSM-CODE iKeys. Note that the HSM menu is only accessible if you are using the ASA 310-FIPS model.

Table 263: HSM Menu Options (/maint/hsm)

Command Syntax and Usage
login *<HSM-USER password for the currently inserted HSM-USER iKey>* Lets you log in to a HSM card, using the HSM-USER iKey and the correct password. After a reboot has occurred (whether intentionally invoked by the user, or due to a power failure for example), the affected ASA 310-FIPS device will not process

Command Syntax and Usage
any SSL traffic until you first log in to the ASA 310-FIPS (with administrator or operator privileges), and then issue the **login** command to log in to the HSM cards. You will then be requested to insert the card-specific HSM-USER iKey, and provide the password that is associated with the inserted HSM-USER iKey. When you have inserted the requested HSM-USER iKeys and provided the associated passwords, alarms that were set during the reboot are cleared. The ASA 310-FIPS device can then start processing SSL traffic again. For detailed information on how to perform this operation, see the section "An ASA HSM Stops Processing Traffic" in the "Troubleshooting the AVG" chapter in the *User's Guide*.
splitkey
Splits the wrap key used by the hardware security module onto the two black CODE iKeys. Prior to performing a split of the wrap key, you are recommended to label the two black CODE iKeys "CODE-SO" and "CODE-USER" respectively, if not already done. When adding an ASA 310-FIPS device to an existing cluster (by selecting **join** in the Setup menu), you will always be asked to insert the CODE-SO and CODE-USER iKeys, in turns, in the HSM cards of the ASA 310-FIPS device you are adding. When installing the very first ASA 310-FIPS device in a new cluster (by selecting new in the Setup menu), you are required to split the wrap key onto the CODE-SO and CODE-USER iKeys. However, should you ever need to split the same wrap key onto a new pair of CODE iKeys (to create backup iKeys for example), you can use the **splitkey** command. **Note:** When the **splitkey** command is used, both the HSM-SO iKey and the HSM-USER iKey that are associated with HSM card 0 are required to perform the operation.
changepass <*card number* **[0|1]**> <*iKey* **[HSM-SO|HSM-USER]**> <*current password for the selected iKey*> <*new password for the selected iKey*>
Sets the password for a HSM-SO or a HSM-USER iKey. After you have specified the desired HSM card and iKey user role, insert the correct iKey in the USB port on the HSM card to which the iKey is associated. Then follow the onscreen instructions. An HSM-SO or a HSM-USER iKey password must be at least 4 characters long and is case sensitive. Spaces are not allowed. **Note:** It is extremely important that you insert the correct HSM iKey when prompted, as the HSM card may otherwise be rendered unusable. Take steps to ensure that the iKey you insert a) belongs to the correct HSM card, and b) corresponds with the iKey user role you specified when prompted. The HSM-SO iKey is purple and embossed with "HSM-SO", while the HSM-USER iKey is blue and embossed with "HSM-USER". Also note that when the HSM-SO iKey password is changed, the HSM-USER is logged out from the HSM card. To resume normal operations after the HSM-SO

Command Syntax and Usage
iKey password has been changed, you will therefore be prompted to insert the HSM-USER iKey and specify the associated HSM-USER password.

/maint/log Logging system configuration

```
[Logging System Menu]

in-memory           - Log in memory
```

Logging information can be cached in internal buffer. The Network devices collects and accesses this information.

/maint/log/in-memory Internal memory configuration

```
[Internal Memory Menu]

onoff       - Set to Enable or Disable Internal Memory.

buffersize  - Set to configure the size of the internal buffer.

displaycfg  - To display the current configuration Settings.
```

All the log messages will be stored in the internal memory.

Table 264: Citrix menu (/cfg/log/in-memory)

Command Syntax Usage
on|off
When set to on, internal memory is enabled. Default value is off.
buffersize
Sets the size of the internal buffer. You can enter the buffer size ranging from 200 to 500.
displaycfg
Displays the following configuration settings:

Command Syntax Usage
• the internal memory status whether it is set to on or off. • the internal memory log status. • maximum message in the memory (which is 300).

Appendix A: CLI Dumps

This appendix includes CLI dumps that are too extensive for display in the Command Reference chapter.

/cfg/dump Configuration Dump

```
>> Configuration#dump

Dump private/secret keys (yes/no) [no]:
Collecting data, please wait...
/*
/*
/* Configuration dump taken Mon June 4 15:17:58 CEST 2012
/* Version 9.0.0.0
/*
/*
/*
/cfg/.
/cfg/ssl/.
/cfg/ssl/server 1/.
name "Redirect to VPN 1"
Alteon iSD SSL
Hardware Platform :3070
Software version: 8.0.0.0
Up time: 2 days 8 mins
IP address: 10.1.82.146
MAC Address: 00:30:48:2e:bf:de
vips 10.1.82.146
standalone off
port "80 (http)"
rip 0.0.0.0
rport 81
type http
proxy on
loopback on
ena enabled
/cfg/ssl/server 1/trace/.
/cfg/ssl/server 1/ssl/.
cert 1
cachesize 4000
cachettl 5m
protocol ssl3
verify none
ciphers ALL@STRENGTH
ena disabled
/cfg/ssl/server 1/tcp/.
cwrite 15m
```

```
ckeep 15m
swrite 15m
sconnect 30s
csendbuf auto
crecbuf auto
ssendbuf auto
srecbuf 6000
/cfg/ssl/server 1/http/.
httpsredir on
redirect on
downstatus unavailable
securecookie off
certcard off
cookieonce off
sslheader on
sslxheader off
sslsidheader off
addxfor off
addvia on
addxisd off
addfront off
addbeassl off
addbeacli off
addclicert off
addnostore off
compress off
cmsie on
rhost off
maxrcount 40
maxline 8192
/cfg/ssl/server 1/http/redirmap/.
/cfg/ssl/server 1/http/dynheader/.
/cfg/ssl/server 1/http/rewrite/.
rewrite off
ciphers HIGH:MEDIUM
response iSD
URI "/cgi-bin/weakcipher"
/cfg/ssl/server 1/http/auth/.
mode basic
realm Xnet
proxy off
ena disabled
/cfg/ssl/server 1/dns/.
/cfg/ssl/server 1/adv/.
/cfg/ssl/server
1/adv/pool/.
timeout 15s
ena disabled
/cfg/ssl/server 1/adv/traflog/.
sysloghost 0.0.0.0
udpport 514
priority info
facility local4
ena disabled
/cfg/ssl/server 1/adv/loadbalancing/.
type all
persistence none
metric hash
health auto
interval 10s
ena disabled
/cfg/ssl/server 1/adv/loadbalancing/script/.
/cfg/ssl/server 1/adv/loadbalancing/remotessl/.
```

```
protocol ssl3
ciphers ALL
/cfg/ssl/server 1/adv/loadbalancing/remotessl/verify/.
verify none
/cfg/ssl/server 1/adv/sslconnect/.
protocol ssl3
ciphers EXP-RC4-MD5:ALL!DH
ena disabled
/cfg/ssl/server 1/adv/sslconnect/verify/.
verify none
/cfg/cert 1/.
name test_cert
cert
-----BEGIN CERTIFICATE-----
MIIEajCCA9OgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBvzELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoT
H1Rlc3QgSW5jLiAxIDEwOjU3OjM4IDIwMDYtMDItMDMxEjAQBgNVBAsTCXRlc3Qg
ZGVwdDEgMB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG
9w0BCQEWGnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMB4XDTA2MDIwMzA5NTcz
OVoXDTA3MDIwMzA5NTczOVowgb8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMRAwDgYDVQQHEwdUZXN0aW5nMSgwJgYDVQQKEx9UZXN0IEluYy4gMSAx
MDolNzozOCAyMDA2LTAyLTAzMRIwEAYDVQQLEwl0ZXN0IGRlcHQxIDAeBgNVBAMT
F3d3dy5kdW1teXNzbHRlc3RpbmcuY29tMSkwJwYJKoZIhvcNAQkBFhp0ZXN0ZXJA
ZHVtbXlzc2x0ZXN0aW5nLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
oH4WLo0VfetyGo1byrPpfIKFeZW2Lx5STmqT/IvxADsW5jOCr672RvyZ+vBUwRuc
2pLauMR0Y87nde3Z9brVVrxReKEVjdltw0hFHEqHB5bE/T6fAjrlo6m1Lz375lXh
wj7Fsv4h9TVQCXIL66q9bPo/+HkzsqAh/jl0u3i0iPsCAwEAAaOCAXIwggFuMAwG
A1UdEwQFMAMBAf8wEQYJYIZIAYb4QgEBBAQDAgJEMDIGCWCGSAGG+EIBDQQlFiNB
bHRlb24vTm9ydGVsIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQUQgLM
A9gz07F2PqiVYnbHQnl8tFwwgewGA1UdIwSB5DCB4YAUQgLMA9gz07F2PqiVYnbH
Qnl8tFyhgcWkgcIwgb8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRAwDgYDVQQHEwdUZXN0aW5nMSgwJgYDVQQKEx9UZXN0IEluYy4gMSAxMDo1Nzoz
OCAyMDA2LTAyLTAzMRIwEAYDVQQLEwl0ZXN0IGRlcHQxIDAeBgNVBAMTF3d3dy5k
dW1teXNzbHRlc3RpbmcuY29tMSkwJwYJKoZIhvcNAQkBFhp0ZXN0ZXJAZHVtbXlz
c2x0ZXN0aW5nLmNvbYIBADAJBgNVHRIEAjAAMA0GCSqGSIb3DQEBBAUAA4GBAHpG
yp1e9cJUgtHv+fn3ygo5QEXJ50Z9/H6WaTqfFe3FpXmDLNJ1xfhldqatYf1Pg6T2
chpv8jqZ4+SxqmxVkcPWm7C5Bp4Sf8owuBsuRc2KLAhRBr3HL3l1k+A0eCNtCFA+
VUx6ASxXUzkNT3a39UuCLP0AKEEAJwfCkQxGfg/d
-----END CERTIFICATE-----
...
/cfg/cert 1/revoke/.
/cfg/cert 1/revoke/automatic/.
anonymous false
interval 1d
ena disabled
/cfg/vpn 1/.
name VPN-1
ips 10.1.82.146
standalone on
/cfg/vpn 1/aaa/.
idlettl 15m
sessionttl infinity
authorder 1
defippool 1
/cfg/vpn 1/aaa/tg/.
ena enabled
recheck 15m
action restricted
details on
loglevel info
/cfg/vpn 1/aaa/tg/agent/.
timeout 2s
minver 0.0.0.0
```

```
/cfg/vpn 1/aaa/wholesec/.
ena false
/cfg/vpn 1/aaa/auth 1/.
type local
name local
/cfg/vpn 1/aaa/auth 1/local/.
/cfg/vpn 1/aaa/auth 1/adv/.
/cfg/vpn 1/aaa/network 1/.
name intranet
/cfg/vpn 1/aaa/network 1/subnet 1/.
net 192.168.0.0
mask 255.255.0.0
/cfg/vpn 1/aaa/network 1/subnet 2/.
net 10.0.0.0
mask 255.0.0.0
/cfg/vpn 1/aaa/network 1/subnet 3/.
net 172.16.0.0
mask 255.240.0.0
/cfg/vpn 1/aaa/service 1/.
name http
protocol tcp
ports 80
/cfg/vpn 1/aaa/service 2/.
name https
protocol tcp
ports 443
/cfg/vpn 1/aaa/service 3/.
name web
protocol tcp
ports 20,21,80,443
/cfg/vpn 1/aaa/service 4/.
name smtp
protocol tcp
ports 25
/cfg/vpn 1/aaa/service 5/.
name pop3
protocol tcp
ports 110
/cfg/vpn 1/aaa/service 6/.
name imap
protocol tcp
ports 143
/cfg/vpn 1/aaa/service 7/.
name email
protocol tcp
ports 25,110,143
/cfg/vpn 1/aaa/service 8/.
name telnet
protocol tcp
ports 23
/cfg/vpn 1/aaa/service 9/.
name ssh
protocol tcp
ports 22
/cfg/vpn 1/aaa/service 10/.
name ftp
protocol tcp
ports 20,21
/cfg/vpn 1/aaa/service 11/.
name smb
protocol tcp
ports 139
/cfg/vpn 1/aaa/service 12/.
```

```
name fileshare
protocol tcp
ports 20,21,139
/cfg/vpn 1/aaa/filter 1/.
name tg_passed
cert ignore
iewiper ignore
tg true
methods ssl,ipsec,netdirect
authservers *
clientnet *
/cfg/vpn 1/aaa/filter 2/.
name tg_failed
cert ignore
iewiper ignore
tg false
methods ssl,ipsec,netdirect
authservers *
clientnet *
/cfg/vpn 1/aaa/group 1/.
name trusted
restrict 0
usertype advanced
idlettl 0
sessionttl 0
vpnadmin false
ippool 0
/cfg/vpn 1/aaa/group 1/access 1/.
network *
service *
appspec *
action accept
/cfg/vpn 1/aaa/group 1/linkset/.
add base-links
/cfg/vpn 1/aaa/group 1/ipsec/.
/cfg/vpn 1/aaa/group 2/.
name tunnelguard
restrict 0
usertype advanced
idlettl 0
sessionttl 0
vpnadmin false
tgsrs srs-rule-test
ippool 0
/cfg/vpn 1/aaa/group 2/linkset/.
/cfg/vpn 1/aaa/group 2/extend 1/.
filter tg_passed
usertype advanced
idlettl 0
sessionttl 0
vpnadmin false
ippool 0
/cfg/vpn 1/aaa/group 2/extend 1/access 1/.
network *
service *
appspec *
action accept
/cfg/vpn 1/aaa/group 2/extend 1/linkset/.
add tg_passed
/cfg/vpn 1/aaa/group 2/extend 2/.
filter tg_failed
usertype
idlettl 0
```

```
sessionttl 0
vpnadmin false
ippool 0
/cfg/vpn 1/aaa/group 2/extend 2/linkset/.
add tg_failed
/cfg/vpn 1/aaa/group 2/ipsec/.
/cfg/vpn 1/aaa/ssodomains/.
add duva.bluetail.com normal
/cfg/vpn 1/aaa/ssoheaders/.
/cfg/vpn 1/aaa/radacct/.
ena false
/cfg/vpn 1/aaa/radacct/servers/.
/cfg/vpn 1/aaa/radacct/vpnattribute/.
vendorid "1872 (alteon)"
vendortype 3
/cfg/vpn 1/server/.
port "443 (https)"
loopback on
ena enabled
/cfg/vpn 1/server/trace/.
/cfg/vpn 1/server/ssl/.
cert 1
cachesize 4000
cachettl 5m
protocol ssl3
ciphers ALL@STRENGTH
verify none
ena enabled
/cfg/vpn 1/server/tcp/.
cwrite 15m
ckeep 15m
skeep 2m
swrite 15m
sconnect 30s
csendbuf auto
crecbuf auto
ssendbuf auto
srecbuf
6000
/cfg/vpn 1/server/http/.
downstatus unavailable
securecookie on
certcard off
cookieonce off
sslheader off
sslxheader off
sslsidheader off
addxfor off
addvia on
addxisd off
addclicert off
addnostore on
compress off
allowimage on
allowdoc off
allowscript off
allowica on
cmsie on
maxrcount 40
maxline 8192
/cfg/vpn 1/server/http/rewrite/.
rewrite off
ciphers HIGH:MEDIUM
```

```
response iSD
URI "/cgi-bin/weakcipher"
/cfg/vpn 1/server/proxymap/.
/cfg/vpn 1/server/portal/.
authenticate on
wipecookies on
cookiedb off
resetcookie off
persistent off
/cfg/vpn 1/server/portal/urlrewrite/.
rewrite on
jrewrite on
cssrewrite on
gziprewrite on
ena enabled
/cfg/vpn 1/server/adv/.
/cfg/vpn 1/server/adv/traflog/.
sysloghost 0.0.0.0
udpport 514
priority info
facility local4
ena disabled
/cfg/vpn 1/server/adv/sslconnect/.
protocol ssl23
ciphers EXP-RC4-MD5:ALL!DH
/cfg/vpn 1/server/adv/sslconnect/verify/.
verify none
/cfg/vpn 1/ipsec/.
ena disabled
cert unset
/cfg/vpn 1/ippool 1/.
type local
name Pool_1
lowerip 10.1.82.148
upperip 10.1.82.149
proxyarp on
ena enabled
/cfg/vpn 1/ippool 1/netattr/.
netmask 255.255.255.0
primnbns 0.0.0.0
secnbns 0.0.0.0
primdns 0.0.0.0
secdns 0.0.0.0
/cfg/vpn 1/portal/.
logintext
This is a configurable text.
...
iconmode fancy
linktext
...
linkurl on
linkcols 2
linkwidth 100%
companyname "Avaya"
smbworkgrp WORKGROUP
applet on
wiper on
ieclear on
citrix off
clientauth off
/cfg/vpn 1/portal/colors/.
color1 #58b2c9
color2 #d0e4e9
```

```
color3 #2088a2
color4 #accdd5
/cfg/vpn 1/portal/content/.
ena disabled
/cfg/vpn 1/portal/faccess/.
ena enabled
ipsecmode native
contip 0.0.0.0
portalmsg
<p>From this page you can gain full network access. This <strong>requires</
strong> that Net Direct is enabled or that you have either Avaya&#039;s
IPSEC client (version 4.89 or better)
and/or SSL-VPN (TDI version 1.1 or better) client installed. If the Net
Direct
installable client is installed it will be used if Net Direct is enabled.</
p>
<p>Note: Your browser must support Java. If not download SUN&#039;s J2SE
JRE from
<a class="white_link"
href="javascript:download_jre()">www.java.com</a>.</p>
<p>Remember: You can only access resources on the network as defined by
your access rights. Contact your network operator if you are dissatisfied
with your current access rights.</p>
...
appletmsg
The quest for full network access has started._The outcome of the quest
will be
indicated in the progress bar and console window below.
...

/cfg/vpn 1/portal/lang/.
setlang en
/cfg/vpn 1/portal/lang/beconv/.
/cfg/vpn 1/portal/whitelist/.
ena disabled
/cfg/vpn 1/portal/whitelist/domains/.
/cfg/vpn 1/portal/blacklist/.
ena disabled
/cfg/vpn 1/portal/blacklist/domains/.
/cfg/vpn 1/linkset 1/.
name base-links
autorun false
/cfg/vpn 1/linkset 1/link 1/.
href "<smb>/xnet/smb/duva.bluetail.com/WORKGROUP/sten"
text "smb link"
type smb
/cfg/vpn 1/linkset 1/link 1/smb/.
/cfg/vpn 1/linkset 1/link 2/.
href <netdirect>
text "Net Direct"
type netdirect
/cfg/vpn 1/linkset 1/link 2/netdirect/.
/cfg/vpn 1/linkset 2/.
name tg_passed

text "The TunnelGuard checks succeeded!"
autorun false
/cfg/vpn 1/linkset 3/.
name tg_failed
text "The TunnelGuard checks failed.<br>Reason:
<var:tgFailureReason><br
>Details: <pre
style=background:#cccccc;><var:tgFailureDetail></pre>"
```

```
autorun false
/cfg/vpn 1/sslclient/.
ippool off
netdirect on
caching off
oslist all
udpports 5000-5001
rekeytraf 0
rekeytime 8h
idlecheck on
clampmss on
splittun enabled_inverse_local
tdiclient off
lspclient off
oldclients false
/cfg/vpn 1/sslclient/splitnets/.
/cfg/vpn 1/adv/.
interface 0
log login
vpnadmin false
usepac true
/cfg/vpn 1/adv/dns/.
search avaya.com
/cfg/vpn 1/adv/dns/servers/.
/cfg/vpn 1/adv/license/.
ssl 0
ipsec 0
/cfg/sys/.
mip 10.1.82.144
/cfg/sys/host 1/.
type master
ip 10.1.82.145
gateway 10.1.82.2
/cfg/sys/host 1/routes/.
/cfg/sys/host 1/interface 1/.
ip 10.1.82.145
netmask 255.255.255.0
gateway 0.0.0.0
vlanid 0
mtu 1500
mode failover
primary 0
/cfg/sys/host 1/interface 1/routes/.
/cfg/sys/host 1/interface 1/ports/.
add 2
/cfg/sys/host 1/port 1/.
autoneg on
speed 0
mode full
/cfg/sys/host 1/port 2/.
autoneg on
speed 0
mode full
/cfg/sys/routes/.
/cfg/sys/time/.
tzone "Europe/Stockholm"
/cfg/sys/time/ntp/.
/cfg/sys/dns/.
cachesize 1000
retransmit 2s
count 3
ttl 3h
health 10s
```

```
hdown 2
hup 2
fallthrough off
/cfg/sys/dns/servers/.
add 10.1.0.10
/cfg/sys/syslog/.
/cfg/sys/accesslist/.
/cfg/sys/adm/.
sonmp off
clitimeout 10m
telnet off
ssh off
/cfg/sys/adm/snmp/.
ena true
versions v1,v2c,v3
/cfg/sys/adm/snmp/snmpv2-mib/.
snmpEnableAuthenTraps disabled
/cfg/sys/adm/snmp/community/.
read public
trap trap
/cfg/sys/adm/snmp/event/.
/cfg/sys/adm/audit/.
vendorid "1872 (alteon)"
vendortype 2
ena false
/cfg/sys/adm/audit/servers/.
/cfg/sys/adm/auth/.
timeout 10s
fallback on
ena false
/cfg/sys/adm/auth/servers/.
/cfg/sys/adm/auth/group/.
vendorid "1872 (alteon)"
vendortype 1
ena false
/cfg/sys/adm/http/.
port 81
ena true
/cfg/sys/adm/https/.
port 443
ena false
/cfg/sys/adm/sshkeys/.
/cfg/sys/adm/sshkeys/knownhosts/.
/cfg/sys/user/.
expire 0
/cfg/lang/.
>> Configuration#
```

/cfg/ssl/server <number> /trace /ssldump SSL Traffic Dump

This command creates a dump of the SSL traffic flowing between clients and the currently selected virtual SSL server. The command is also available for portal servers (**/cfg/vpn <id>/server/trace/ssldump**).

Below is an example of SSL traffic captured for a portal server.

```
>> >> Trace# ssldump

ssldump flags [-n -A -d -i eth1]:
ssldump filter [tcp and port 443 and ((host 10.1.82.146))]:
Output mode (interactive/tftp/ftp/sftp) [interactive]:


Note that ssldump cannot decrypt any traffic if it is
started after the browser. It need to be running during
the initial SSL handshake.
Hit <return> to end dump
New TCP connection #1: 192.168.128.19(2975) <-> 10.1.82.146(443)
1 1  0.0014 (0.0014)  C>SV3.0(97)  Handshake
ClientHello
Version 3.0
random[32]=
41 7d 0f 75 d3 18 96 5b 2d ef 13 20 74 a2 dd 94
cf d9 5b a1 cf cf f6 74 8f 2c 5c 28 f5 84 33 4d
resume [32]=
f6 39 71 b9 ca cd 99 c0 29 9a ec aa 93 b2 64 d6
49 ca db 70 84 76 37 d4 f2 47 5e d5 7b 44 54 1d
cipher suites
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
compression methods
NULL
New TCP connection #2: 192.168.128.19(2976) <-> 10.1.82.146(443)
2 1  0.0010 (0.0010)  C>SV3.0(97)  Handshake
ClientHello
Version 3.0
random[32]=
41 7d 0f 75 6b 66 6e a4 a4 14 6a 87 5f 10 e7 07
e4 bf 27 86 fe 45 ae a2 e4 92 d3 93 42 40 b9 9a
resume [32]=
f6 39 71 b9 ca cd 99 c0 29 9a ec aa 93 b2 64 d6
49 ca db 70 84 76 37 d4 f2 47 5e d5 7b 44 54 1d
cipher suites
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5
SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
compression methods
NULL
```

```
1 2  0.0026 (0.0012)  S>CV3.0(74)  Handshake
ServerHello
Version 3.0
random[32]=
41 7d 0e 10 d1 92 1d 56 f1 c1 6f 4f 03 26 c5 39
04 8d 6a 2f 2f 46 fd 80 c5 6d 15 62 cc ea 70 61
session_id[32]=
f6 39 71 b9 ca cd 99 c0 29 9a ec aa 93 b2 64 d6
49 ca db 70 84 76 37 d4 f2 47 5e d5 7b 44 54 1d
cipherSuite   SSL_RSA_WITH_RC4_128_MD5
compressionMethod NULL
1 3  0.0026 (0.0000)  S>CV3.0(1)  ChangeCipherSpec
1 4  0.0026 (0.0000)  S>CV3.0(56)  Handshake
2 2  0.0023 (0.0013)  S>CV3.0(74)  Handshake
ServerHello
Version 3.0
random[32]=
41 7d 0e 10 59 39 7b 3d 26 1b 55 64 cf f7 36 61
84 c0 f2 0e 22 f3 a7 6f 8d 15 e5 8e 01 b8 1c 66
session_id[32]=
f6 39 71 b9 ca cd 99 c0 29 9a ec aa 93 b2 64 d6
49 ca db 70 84 76 37 d4 f2 47 5e d5 7b 44 54 1d
cipherSuite   SSL_RSA_WITH_RC4_128_MD5
compressionMethod NULL
2 3  0.0023 (0.0000)  S>CV3.0(1)  ChangeCipherSpec
2 4  0.0023 (0.0000)  S>CV3.0(56)  Handshake
1 5  0.0037 (0.0011)  C>SV3.0(1)  ChangeCipherSpec
1 6  0.0037 (0.0000)  C>SV3.0(56)  Handshake
1 7  0.0053 (0.0015)  C>SV3.0(348)  application_data
2 5  0.0047 (0.0023)  C>SV3.0(1)  ChangeCipherSpec
2 6  0.0047 (0.0000)  C>SV3.0(56)  Handshake
2 7  0.0058 (0.0010)  C>SV3.0(550)  application_data
1 8  0.0263 (0.0209)  S>CV3.0(328)  application_data
1 9  0.0264 (0.0001)  S>CV3.0(21)  application_data
1 10 0.0285 (0.0021)  C>SV3.0(339)  application_data
1 11 0.0294 (0.0008)  S>CV3.0(331)  application_data
1    0.0297 (0.0002)  S>C  TCP FIN
1    0.0304 (0.0007)  C>S  TCP FIN
2    0.0895 (0.0837)  S>C  TCP FIN
2    0.0902 (0.0007)  C>S  TCP FIN
```

/cfg/ssl/server <number> /trace /tcpdump TCP Traffic Dump

This command creates a dump of the TCP traffic flowing between clients and the currently selected virtual SSL server. The command is also available for portal servers (**/cfg/vpn <id>/server/trace/tcpdump**).

Below is an example of TCP traffic captured for a portal server.

```
>> Trace# tcpdump

tcpdump flags [-s 0 -n -v -i eth1]:
```

```
tcpdump filter []:
Output mode (interactive/tftp/ftp/sftp) [interactive]:
Output mode (binary/ascii) [ascii]:
Hit <return> to end dump
16:45:13.391130 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:13.985220 arp who-has 10.1.82.102 tell 10.1.82.2
16:45:14.400607 arp who-has 10.1.82.122 tell 10.1.82.2
16:45:15.414149 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:16.421807 arp who-has 10.1.82.122 tell 10.1.82.2
16:45:17.433610 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:18.282990 IP (tos 0x0, ttl  64, id 86, offset 0, flags [DF], length:
45) 1
0.1.82.145.1087 > 10.1.0.10.53: [udp sum ok]  0 NS? . (17)
16:45:18.288721 IP (tos 0x0, ttl  63, id 65172, offset 0, flags [none],
length:
256) 10.1.0.10.53 > 10.1.82.145.1087: [udp sum ok]  0 0/13/0 (228)
16:45:18.443475 arp who-has 10.1.82.122 tell 10.1.82.2
16:45:19.455806 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:20.464597 arp who-has 10.1.82.122 tell 10.1.82.2
16:45:21.476492 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:22.486173 arp who-has 10.1.82.122 tell 10.1.82.2
16:45:23.498518 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:24.507664 arp who-has 10.1.82.122 tell 10.1.82.2
16:45:25.519360 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:26.528842 arp who-has 10.1.82.122 tell 10.1.82.2
16:45:27.541346 arp who-has 10.1.82.121 tell 10.1.82.2
16:45:28.292956 IP (tos 0x0, ttl  64, id 87, offset 0, flags [DF], length:
45) 1
0.1.82.145.1087 > 10.1.0.10.53: [udp sum ok]  0 NS? . (17)
16:45:28.293998 IP (tos 0x0, ttl  63, id 65210, offset 0, flags [none],
length:
```