Troubleshooting Guide
Avaya VPN Gateway

8.0
NN46120-700, 04.02
December 2010

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

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

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: New in this release

The following section detail what's new in *Avaya VPN Gateway Troubleshooting Guide* (NN46120-700) for Release 8.0.

Features

See the following sections for information about feature changes:

Log files

This section is updated to provide information about the IPSec debug command. For more information about log files, see Log files on page 14.

Viewing IKE internal information

This section is added to explain how to view IKE internal information. For more information about viewing IKE internal information, see Viewing IKE internal information on page 20.

Troubleshoot IPSec

This section is added to provide information about troubleshooting issues related to IPsec. For more information about IPsec troubleshooting, see Troubleshoot IPsec on page 23.

Troubleshoot Net Direct

This section is updated to provide information about troubleshooting issues related to Net Direct. For more information about Net Direct troubleshooting, see Troubleshoot Net Direct on page 28.

Troubleshoot software upgrade issues

This section is added to provide information about troubleshooting issues related to software upgrades. For more information about software upgrade troubleshooting, see Troubleshoot software upgrade issues on page 34.

Troubleshoot Secure Portable Office Client

This section is updated to provide information about the Ceedo log utility and issues that occur when you abruptly unplug the USB.

For more information about the Ceedo log utility, see Activating and using Ceedo log utility on page 39.

For more information about troubleshooting USB-related issues, see Troubleshooting Delayed Write Failed issue on page 39.

Troubleshoot cluster joining issue

This section is added to provide information about troubleshooting issues related to cluster joining. For more information about cluster joining troubleshooting, see Troubleshoot cluster joining issues on page 39.

Troubleshoot L2TP/IPSec issues

This section is added to provide information about troubleshooting issues related to L2TP/IPSec. For more information about L2TP/IPSec troubleshooting, see Troubleshoot L2TP/IPsec issues on page 40.

Troubleshoot Web Rewrite issue

This section is added to provide information about troubleshooting issues related to Web Rewrite. For more information about Web Rewrite troubleshooting, see Troubleshoot Web Rewrite issue on page 42.

Other Changes

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

- The Emergency Recovery Trees chapter is updated with Cannot access SSL VPN Portal — recovery tree. For more information, see Cannot access SSL VPN Portal — recovery tree on page 71
- The Emergency Recovery Trees chapter is updated with Cannot access IPsec VPN — recovery tree. For more information, see Cannot access IPsec VPN — recovery tree on page 72.
- The Emergency Recovery Trees chapter is updated with Reimage AVG — recovery tree. For more information, see Reimage AVG — recovery tree on page 74.
- The recovery tree of Cannot access AVG for management is updated in chapter Emergency Recovery Trees. For more information, see Cannot access AVG for management — recovery tree on page 69

Chapter 2: Introduction

This chapter describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway (AVG). Use the troubleshooting tools to enhance overall performance, resolve error messages, and increase response time for a specific feature.

Each tool is described by purpose, usage procedures, and how to interpret the output.

Prerequisites

Avaya recommends you to use one or more of the following commercially available troubleshooting tools as well as the tools described in this document.

- Capture and analyze HTTP and HTTPS with the HTTP Analyzer from IE Inspector http://www.ieinspector.com/
- Capture and analyze HTTP and HTTPS with Tamper Data, a plug-in available for Mozilla Firefox https://addons.mozilla.org/en-US/firefox/addon/966
- Display the time to load Web pages with Faster Fox, a plug-in available for Mozilla Firefox https://addons.mozilla.org/en-US/firefox/addon/1269
- Capture and analyze packets with either Sniffer or Wireshark from Network General http://www.wireshark.org/ and http://www.networkgeneral.com/

Navigation

Chapter 3: Troubleshooting Fundamentals

This section provides conceptual information about the methods and tools that you can use to troubleshoot and isolate problems in the Avaya VPN Gateway.

Navigation

SSL acceleration

The Secure Sockets Layer (SSL) protocol runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client. The client then authenticates itself to the server, and both machines establish an encrypted connection. The current standard is TLS (Transport Layer Security) but the name SSL is still used.

See Dumping the log files to another server on page 19 for instructions on how to view the ssl.log files.

Table 1: Interpreting SSL acceleration log files on page 13 gives the information about log files messages and their descriptions.

Table 1: Interpreting SSL acceleration log files

Message	Severity	Type	Description
Failed to initialize SSL hardware	ERROR	Traffic processing	The SSL acceleration hardware failed to initialize and the AVG runs with degraded performance.

Message	Severity	Type	Description
Set CSWIFT as default	INFO	Startup	The AVG is using CSWIFT SSL hardware acceleration.
ssl-hw-fail	ALARM (MAJOR)	System control	The SSL hardware acceleration card could not be found or initiated and the AVG runs with degraded performance.
Using <hardware type> hardware	INFO	Startup	The AVG is using <hardware type> hardware for SSL acceleration.

Log files

View the log files to see the history of system events.

This troubleshooting guide documents only the most common messages from the ssl.log.

Simpleproxy

```
/maint/debug/proxydebug [on|off|once]
```

on: enables Simpleproxy to print out debug message.

off: disables Simpleproxy to print out debug message.

once: enables Simpleproxy to print out debug message only once.

IPsec

```
    /maint/debug/iketrace [off |error | warning | important | geninfo |
funcentryexit]
```

off: sets the trace level to off.

error: sets the new trace level to error.

warning: sets the new trace level to warning.

important: sets the new trace level to important.

geninfo: sets the new trace level to general information.

funentryexit: sets the new trace level to function enter-exit.

Important:

Enabling debug message uses more CPU resource. Make sure to disable it after you finish debugging.

Transmit the event log from the Avaya VPN Gateway to a file on a TFTP, FTP, or SFTP server. Specify the IP address or host name of the server as well as the file name. The default value is TFTP.

Table 2: Log file types in a log dump on page 15 lists the log file types in a log dump.

Table 2: Log file types in a log dump

Log file type	Description
clierror	This log provides information on the CLI engine and is used by engineering to debug issues.
erlerror	This log provides information on the applications in Erlang virtual machine.
erlstart	This log provides information on the internal Erstart language engine and SSL acceleration. It is used by Engineers to debug issues while in development.
conslog	This log contains messages displayed on the console port of the device. These messages are the one that are generated during boot sequence. These messages are generated during boot sequence.
dmesg	This log contains messages generated by the kernel.
ssl.log	This log contains messages generated by the simpleproxy features.
ikelog	IPsec module related messages.
message	This log contains standard syslog types of messages and contains general information such as system-level status and non-application acceleration errors across the device.

Traffic Generators

Use the traffic dump commands to display either the SSL or TCP traffic capture tools in the system.

Table 3: Interpreting an SSL traffic dump on page 16provides information on SSL dump entry and its description.

Table 3: Interpreting an SSL traffic dump

Dump entry	Description
New TCP connection #<connection number>: <sending host IP> (<port number>) <-> <receiving host IP>(<port number>)	A new TCP connection <number> made between the sending host using port <number> to the receiving host using port <number>.
<connection number> <start timestamp> (<previous record timestamp>) S>C <record type> FIN	The timestamp when the connection occurred and the elapsed time since the last connection. The connection is from server to client (S>C) or client to server (C>S) and is a record type.

Table 4: Interpreting an TCP traffic dump on page 16 gives the information about TCP dump entry and its description.

Table 4: Interpreting an TCP traffic dump

Dump entry	Description
<ID number> IP <source IP and port>> <destination IP and port>: <flags><data sequence number> ack <sequence number of next data> win <window number> Urg <tcp options>	It is a TCP connection between a source and destination. Flag values are S (SYN), F (FIN), P (PUSH), R (RST), or a single period (no flags). The data sequence space covered by the data in this packet. Ack is the sequence number of the next data expected in the other direction on this connection. Window number is the number of bytes of receive buffer space available in the other direction on this connection. Urg indicates there is urgent data in the packet. TCP options are enclosed in angle brackets.

AVG hardware

This section provides information to troubleshoot problems related to the Avaya VPN Gateway hardware components.

Table 5: Front Panel LEDs on page 16 describes the Front Panel LED indicators on the VPN Gateway.

Table 5: Front Panel LEDs

LED Indicator (from left to right)	Description
Amber system status LED	The amber system status LED lights up when the system needs attention due to a problem with

LED Indicator (from left to right)	Description
	power supplies, fans, CPU, or system temperature.
Hard-disk drive activity LED	This LED blinks when activity is detected on the hard-disk drive.
System power LED	This LED is green when the power supply is turned on.

Important:
Call Avaya for RMA if Amber System status LED can not be cleared.

Virtual IP addresses

In instances where virtual IP addresses are used without an external load balancer, ensure that the effected services are set to standalone mode by running **`/cfg/vpn #/standalone on`** command.

Chapter 4: Global troubleshooting tasks

This section describes the global troubleshooting tools available at the operating system level.

Navigation

Dumping the log files to another server

Perform the following procedure to dump the log files to another server.

Procedure steps

1. From the command line, enter this command.

   ```
   /maint/dumplogs
   ```

2. Enter the transfer protocol (tftp, ftp, or sftp).
3. Enter the host name or IP address of the target server.
4. Enter the name of the file to be dumped to the target server. The filename must have an extension of .tgz. The file is an archive file, bundled with tar, and compressed with gzip.
5. Confirm that the dump collects information from all the hosts in the cluster.
6. If using FTP, enter the user name and password.
7. Use a newer version of WinZip to unpack the file on the targeted server.
8. Use the following table to identify the types of log files in a dump.

Displaying the audit trials

Use this tool to view changes in the system. The audit trial must be used in conjunction with the system.

Procedure steps

1. From the command line, enter this command to add an audit server to the device.

   ```
   /cfg/sys/adm/audit/servers/add <IP address> <udp-port>
   <shared server password>.
   ```

2. From the command line, enter this command to enable audit logging.

   ```
   /cfg/sys/adm/audit/ena.
   ```

3. All configuration changes are sent to the RADIUS.

Following are the tips to implement SSL acceleration.

- Make sure your system is configured for SSL acceleration.
- Use browsers on the client machines that are capable of doing HTTPS.

Viewing SSL traffic generators

Perform the following procedure to view SSL traffic generators.

Procedure steps

From the command line, enter this command to view the SSL traffic dump.

```
/cfg/vpn # /server/trace/ssldump
```

Viewing IKE internal information

Perform the following procedure to view IPsec IKE internal information.

Procedure steps

From the command line, enter this command to view the internal information of IPsec IKE.

```
/maint/debug/ikedump
```

Viewing TCP traffic generators

Perform the following procedure to view SSL traffic generators.

Procedure steps

From the command line, enter this command to view the TCP traffic dump.

```
/cfg/vpn # /server/trace/tcpdump
```

Chapter 5: Feature-specific troubleshooting tasks

This section describes the feature-specific troubleshooting tools available at the operating system level.

Navigation

Troubleshoot IPsec

This section explains the steps to troubleshoot IPsec-related issues. The following issues can occur:

- new IPsec connection reject
- massive IPsec session drop
- authentication failure

Establishing an IPsec connection issue

Perform the following procedure to troubleshoot the issues related to establishing an IPsec connection. These issues can occur due to the following reasons:

- license exhaustion
- IP pool exhaustion

Procedure steps

1. Enter this command to check the IPsec/SSL license.

   ```
   /info/license
   ```

2. Enter this command to check the IP pool usage.

   ```
   /info/ippool
   ```

3. Enter this command to check the aged IPSec users.

   ```
   /info/users ipsec
   ```

4. Enter this command to enable the Initial Contact Payload to override existing session.

   ```
   /cfg/vpn #/ipsec/icp on
   ```

Alternatively, you can perform the following procedure to troubleshoot the issue.

Procedure steps

1. Enter this command to collect the AVG server log.

   ```
   /maint/dumplog
   ```

2. Enter this command to collect the AVG status log.

   ```
   /maint/dumpstat
   ```

3. Enter this command to forcefully log off the aged users.

   ```
   /info/kick
   ```

4. Restart the device.
5. Check for the latest release note for known issue or resolved issue.

Troubleshooting massive IPsec session drop issues

Perform the following procedure to troubleshoot the issues related to a massive IPsec session drop. These issues can occur due to the following reasons:

- IKE daemon crash
- device restart

Procedure steps

1. Enter this command to collect the AVG server log.

   ```
   /maint/dumplog
   ```

2. Enter this command to collect the AVG status log.

   ```
   /maint/dumpstat
   ```

3. Log on as the root user.
4. Run the "last" command to identify the device reboot timestamp and restart type.
5. Enable the IKE core dump process.
6. Check for the latest release note.

Alternatively, you can perform the following procedure to troubleshoot this issue.

Procedure steps

1. Enter this command to enable iketrace to funcentryexit.

   ```
   /maint/debug/iketrace funcentryexit
   ```

   Important:

   Enabling debug message uses more CPU resource. Make sure to disable it after you finish debugging.

2. Log on as the root user, and then dump the SADB and SPD database using the following commands.

   ```
   setkey -DP setkey -D
   ```

   The command output appears on the screen. The administrator must capture the output and provide the details to the Avaya support engineer.

Troubleshooting IPSec authentication issue

Perform the following procedure to troubleshoot the issues related to IPSec authentication. These issues can occur due to the following reasons:

- password mismatch due to language set problem
- backend authentication server issue
- the **/cfg/vpn #/ipsec/groupmatch** configuration issue

Procedure steps

1. Enter this command to collect the AVG server log.

   ```
   /maint/dumplog
   ```

2. Enable `/maint/starttrace`, and then capture trace message.
3. Enter these commands to check the language set of the server and client.

   ```
   /cfg/lang  /cfg/vpn #/portal/lang
   ```

4. Check for the latest release note.

Alternatively you can perform the following procedure to resolve this issue.

Procedure steps

Enter this command to increase the CPU load.

```
maint/debug/iketrace funcentryexit
```

OR

Enter this command to disable groupmatch.

```
/cfg/vpn #/ipsec/groupmatch false
```

Troubleshooting core file generation

Perform the following procedure to rectify the issues related to generating the core file.

Procedure steps

1. Log on as the root user.
2. Enter this command to generate the core file when IKE daemon crashes.

   ```
   touch /tmp/ikecore
   ```

3. Enter this command to generate the core file only once.

   ```
   touch /tmp/ikecoreonce
   ```

You can view the core file under /logs directory.

Troubleshooting SSL acceleration

Perform the following procedure to troubleshoot SSL acceleration. These steps uses the troubleshooting tools described in this section. See Displaying Traffic Generators VPN Command Line Interface Guide (NN46120-101) for commands not covered in this document.

Procedure steps

1. Make sure SSL acceleration is enabled for the service.
2. View the output from the ssldump for the service. See for the ssldump command.

SSL acceleration troubleshooting tools

Use the traffic load data and SSL acceleration-specific error messages to troubleshoot SSL acceleration.

SSL acceleration troubleshooting tools navigation

- Viewing current configuration on page 27
- Resetting default configuration on page 27

Viewing current configuration

Perform the following procedure to view current configuration.

Procedure steps

From the command line, enter this command

`/stats/sslstats/server #` is the host number associated with the current SSL acceleration service.

Resetting default configuration

To remove all configuration settings from the Avaya VPN Gateway, use the **`/boot/delete`** command. This command resets the system to the default settings.

Procedure steps

From the command line, enter this command.

```
/boot/delete
```

Important:
After you enter this command, you must log in to the AVG and perform the initial setup.

Troubleshoot Net Direct

For troubleshooting Net Direct, retrieve the following Net Direct log files from the client machine. These log files are located in the users temp folder (%TEMP%).

- netdirect.log
- netdirectrunner.log
- netdirectocx.log
- tapinstall.log
- ConNDLog.log

The following issues can occur:

- Unstable Net Direct connectivity issue
- Crashing Net Direct in end-user PC
- High CPU utilization in end-user PC

Troubleshooting unstable Net Direct connectivity issues

Perform the following procedure to rectify the issues related to unstable Net Direct connectivity. These issue can occur due to the following reasons:

- Simpleproxy failure
- Tunnel Guard failure
- End user wireless router issue

To resolve this issue restart the end user wireless router.

If the problem still exists, perform the following procedure.

Procedure steps

1. Check for the latest release notes.
2. Collect the Net Direct log from the client PC.

3. Enable the following command, and capture the trace message.

   ```
   /maint/starttrace
   ```

4. Enter this command to collect the AVG server log.

   ```
   /maint/dumplog
   ```

5. Run a packet trace tool like Wireshark in the end user PC and TCP dump in the AVG server to collect the packet capture.

Troubleshooting Net Direct crash issues

Perform the following procedure to resolve the issue related to crashing Net Direct in a user PC. These issues can occur due to the following reasons:

- version compatibility issue of cached client
- installation issue
- operation system compatibility issue

Procedure steps

Check for the cached Net Direct, and then delete the cached Net Direct.

OR

Uninstall the client from the PC, and then reinstall the client.

Alternatively, you can perform the following procedure.

Procedure steps

1. Check for the latest release notes.
2. Collect the Net Direct logs.
3. Enable the following command, and then capture the trace message.

   ```
   /maint/starttrace
   ```

4. Run the following command to collect the AVG server log.

   ```
   /maint/dumplog
   ```

Troubleshooting high CPU utilization issues

Perform the following procedure to rectify the issues related to high CPU utilization in a user PC. These issues can occur due to the following reasons:

- bad certificate
- operation system compatibility issue

Procedure steps

1. Check for the latest release notes.
2. Collect the Net Direct logs.
3. Enable the following command, and then capture the trace message.

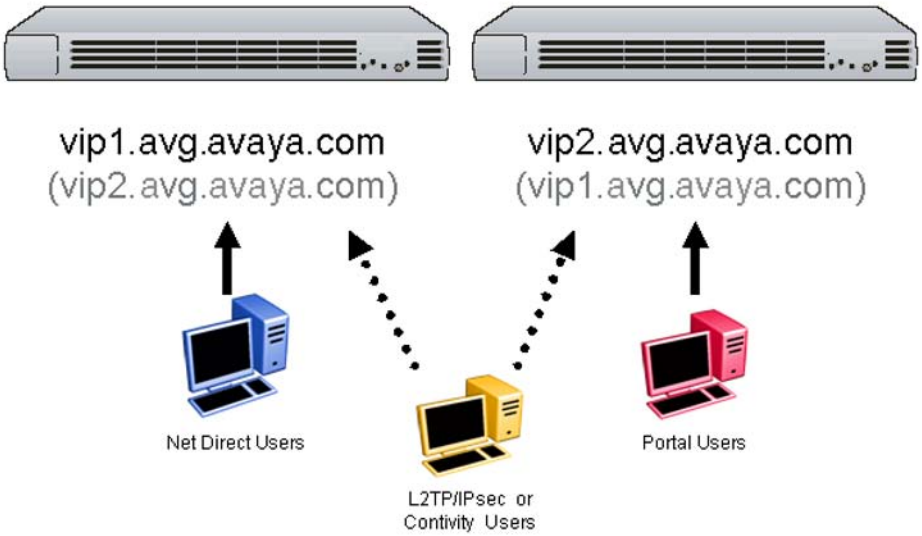
   ```
   /maint/starttrace
   ```

Separating Net Direct service and Portal service

Net Direct and Portal session are handled by one single process. The instability issue of Portal session can affect the Net Direct session. To provide service continuity and minimize the impact of debugging the Portal issue to Net Direct users, the administrator can setup two VPNs in the cluster system to serve each service. A single cluster system provides a single system image management but two different traffic handlers. If one node goes down, the surviving node still serves both the Net Direct and the Portal modes to provide fault-tolerance. The Portal issue does not affect L2TP and Contivity IPSec. The minimum requirements for separating Net Direct and Portal services are as follows:

- two-host clustered system
- two DNS names for each VPN
- two VIPs

The following figure shows the Net Direct and Portal service deployment configuration:



Perform the following procedure to separate the Net Direct service and Portal service.

Procedure steps

1. Remove the load balancer, if any.
2. Remove the DNS Round Robin, if any.
3. Add a DNS name for Portal access or Net Direct access.
4. Add a VIP in AVG.
5. Deploy the DNS name to the Net Direct or Portal user to separate the traffic.

Troubleshooting TunnelGuard

Perform the following procedure to troubleshoot the TunnelGuard Installed Agent issues.

1. Enable debug logging on AVG/AVR.

   The debugging information is used to track the errors in the TunnelGuard SRS rules.
2. Enter the following command to debug the information from the TunnelGuard applet.

   `cfg/ vpn #/aaa/ tg/ loglevel debug.`
3. Enter apply.
4. Add agent.lcf in the path `<TG-Install-Dir>\resources` directory.
5. Restart the system.
6. Collect TunnelGuard logs from `<TG-Install-Dir>log` directory.

   Important:
   The default path to access TG-Install-Dir is `C:\Program Files\Nortel Networks\TunnelGuard\`.
7. Attach these logs to the CR.
8. For all users, attach Profiles.ini from `%ALLUSERSPROFILE%\Application Data \Nortel Networks\TunnelGuard` directory.

   Important:
   The default profile path for all users is `C:\Documents and Settings\All Users`.
9. For logged in users, attach Profiles.ini from `%APPDATA%\Nortel Networks \TunnelGuard` directory.

   Important:
   You can attach Profile.ini for both 'all users' and 'logged in users' if it is available in their respective paths.

Important:

The default profile path for logged in users is `C:\Documents and Settings\<user>`.

Perform this procedure to troubleshoot the TunnelGuard Applet issues.

1. Enable debug logging on AVG/AVR.

   The debugging information is used to track the errors in the TunnelGuard SRS rules.

2. To debug the information from the TunnelGuard applet, enter the following command.

   ```
   cfg/ vpn #/aaa/ tg/ loglevel debug
   ```

3. Enter apply.
4. Open Java console from IE Tools->Sun Java Console.
5. Copy all the logs in a text file.
6. Attach these logs to the CR.

Recovering using boot.img

When you log in as the boot user and perform a reinstallation of the software, the VPN Gateway is reset to its factory default configuration. All configuration data and current software is wiped out, including old software image versions or upgrade packages that may be stored in the flash memory card or on the hard disk. Also note that a reinstall must be performed on each VPN Gateway through a console connection.

A reinstall wipes out all configuration data (including network settings). Therefore you should first save all configuration data to a file on a TFTP/FTP/SCP/SFTP server. Using the ptcfg command, installed keys and certificates are included in the configuration data, and can later be restored by using the gtcfg command.

To reinstall a VPN Gateway, you need the following:

- Access to the VPN Gateway through a console connection.
- An install image, loaded on a FTP/SCP/SFTP server on your network.
- The IP address of the FTP/SCP/SFTP server.
- The name of the install image.
- Log in as user: boot.

When performing a reinstallation of the AVG software, access to the VPN Gateways must be accomplished through the console port.

Procedure steps

1. Log in as the boot user and provide the correct password.
2. Confirm the network port setting, and the IP network settings.

   If the VPN Gateway has not been configured for network access previously, or if you have deleted the VPN Gateway from the cluster by using the `/boot/delete` command, you must provide information about network settings such as interface port, IP address, network mask, and gateway IP address. No suggested values related to a previous configuration will be presented within square brackets.
3. Select a download method, specify the server IP address, and the boot image file name.

   If the FTP server does not support anonymous login, enter the required FTP user name and password. Anonymous login is the default option.
4. Log in to the VPN Gateway as the admin user, after the device has rebooted on the newly installed boot image.

   After the new boot image has been installed, the VPN Gateway will reboot and you can log in again when the login prompt appears. This time, log in as the admin user to enter the Setup menu.

Upgrading code using .pkg

The Avaya VPN Gateway (AVG) software image is the executable code running on the VPN Gateway. A version of the image ships with the VPN Gateway, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your VPN Gateway.

To upgrade the VPN Gateway, you need the following:

- Access to one of your VPN Gateways through a remote connection (Telnet or SSH), or a console connection.
- The software upgrade package, loaded on a FTP/SCP/SFTP server on your network.
- The host name or IP address of the FTP/SCP/SFTP server. If you choose to specify the host name, note that the DNS parameters must have been configured.
- The name of the software upgrade package (upgrade packages are identified by the .pkg file name extension).

When you have gained access to the VPN Gateway, use the following procedure.

Procedure steps

1. To download the software upgrade package, enter the following command at the Main menu prompt. Then select whether to download the software upgrade package from a FTP/SCP/SFTP server.

```
>> Main# boot/software/download
Select protocol (ftp/scp/sftp) [ftp]: ftp
```

2. Enter the host name or IP address of the server.

```
Enter hostname or IP address of server: <server host
name or IP>
```

3. Enter the file name of the software upgrade package to download.

```
Enter filename on server: <filename.pkg>
FTP User (anonymous): <username or press ENTER for
anonymous mode>
Password: <password or press ENTER for default
password in anonymous mode>
Received 28200364 bytes in 4.0 seconds

Unpacking...
ok

>> Software Management#
```

If needed, the file name can be prefixed with a search path to the directory on the FTP/SCP/SFTP server.

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/IP.isd.

Troubleshoot software upgrade issues

This section explains how to troubleshoot issues related to software upgrades. The following issues can occur:

- unpacking software failure
- VPN log on

Troubleshoot software unpacking failure issue

The AVG stores the applications extracted from the software image in the /isd file system. You must ensure that the file system has ample space to hold two software images. If you have

allocated limited space in the /isd file system, you can encounter problem in unpacking the software.

Due to the increased size of the AVG in Release 7.x to 8.0, you must increase the size of the existing file system using the disk repartitioning command. Run the following commands to repartition the hard disk:

- `/boot/repartition` initiates repartitioning for the local host
- `/cfg/sys/host <id>/repartition /cfg/sys/cluster/host <id>/repartition` initiates repartitioning for the given running host

These commands are hidden, and do not appear in the menu. These commands are not considered for auto-completion through <TAB>; you cannot use them in normal operation. Repartition includes two automatic restarts, and takes the host effectively out of service. You require approximately five to seven minutes for the repartition.

Troubleshooting VPN login with LDAP authentication server issues

Important:

This troubleshooting is applicable only when you upgrade the software to AVG 8.0.

After upgrading the AVG from 7.x to release 8.0, if you cannot log on to the VPN using Portal, ND, IPSec client, or L2TP client with the LDAP authentication server, perform the following procedure.

Procedure steps

Ensure that the servers are configured in

`/cfg/vpn #/aaa/auth #/ldap/servernames`.

- If the servers are not configured, configure the `/cfg/vpn #/aaa/auth #/ldap/servernames` with the same information as in `/cfg/vpn #/aaa/auth #/ldap/servers`. The `servernames` ask for the Netbios name in addition to the server name and the LDAP port.
- If the servers are configured, enable `/main/starttrace` with the aaa module. The traces gives the reason for the failure.

In the AVG Release 8.0, you cannot use the servers configured under `/cfg/vpn #/aaa/auth #/ldap/servers` for authentication. The `/cfg/vpn #/aaa/auth #/ldap/servernames` should be configured for the authentication servers.

Troubleshoot Secure Portable Office Client

To troubleshoot Secure Portable Office (SPO) Client, you need to get the log file SPOClient.log from one of the following devices:

- U3P
- CD ROM
- Generic USB

This log file is located in the USB device inside SPOClient folder. For information on SPOlog file, see SPO Client on page 97.

Different log levels can be enabled using the Dashboard Tools->Preference.

For information on the various preferences see, *Avaya Configuration - Secure Portable Office (SPO) Guide, (NN46120-301)*.

Secure Portable Office messages

This following table shows different messages, causes, and actions that need to be taken to rectify the issues of the SPO client:

Table 6: SPO Messages

Message	Cause	Action
Not Authorized for using SPOClient	In AVG server the user group is not enabled for **`spoaccess`** .	Check with administrator on the access group.
The SPO client did not receive a correct response from the VPN Gateway. Please try again or contact your VPN administrator	SPO Client connected to wrong server that is, server image is not capable of handling SPO Client.	Try connecting to the server using Web browser or contact VPN administrator.
Could not establish SSL connection, check whether valid certificate is used	Invalid certificate selected when user is prompted to present the client certificate or check the certificate properties if it is not expired.	Use valid certificate or request valid certificate from the VPN administrator.

Message	Cause	Action
Authentication failed	Incorrect login username or password.	Provide valid username and password.
Authentication failed	VPN Gateway exceeded total number of users allowed by license.	Try reconnecting later or contact VPN administrator.
Connection failed	VPN Gateway is down and not reachable.	Contact the VPN administrator.
Password Mismatch	New Password and Confirm password fields didn't match.	Ensure that New Password and Confirm Password match.
Your Password will expire in "n" Days	Password will expire in "n" days	Change the password through Change Password under Tools->ChangePassword in Dashboard.
Failed to load Virtual Desktop	Vdesktop did not load properly	Check if Vdesktop is enabled on the server. Check if stable version of Vdesktop is available on the server.
Error Moving SpoClient application to Vdesktop	Unable to start SPOClient in Vdesktop.	Change in Vdesktop Library.
A Corrupt "Softwarename" was received.	Do you want to try downloading again Software file was modified along the route.	Ensure that files are not modified along the path by any networking elements.
You Can't Update Base software.	In case CD-Rom based client, Base Software upgrade is not supported.	For CD-Rom based SPOClient. We will have to make a new copy of the CD.
Invalid Session-Restarting the application	Session was removed from the server.	In the server under **`/info/users`**. See if the user session still exists.
User Link "UserLinkName" Not Added.	Please Verify Path User Link was not added as the user link didn't exist in the specified path.	Copy the corresponding application in the specified path.
Unable To bind. Cannot start Custom App	Port Forwarder didn't Start.	Ensure JRE is present, PortForwarder was started.
Cannot start PostForwarder-Port is already Binded.	Unable to Start Port Forwarder as Port is already Binded	Specify a different Port.

Message	Cause	Action
Vdesktop not Enabled on	Server Vdesktop is not enabled on the server.	In the Server **/cfg/vpn #/vdesktop/**Enable it
Failed to Run NetDirect.exe	Unable to start NetDirect.	Check whether you have NetDirect.exe on the specified path.
NetDirect can't be started when DHCP client service is not running	DHCP client service is not running on the client machine.	Start the DHCP client service and try to launch the NetDirect again.
Can not start NetDirect.Contivity is running on this machine	Contivity VPN client is running.	Stop contivity client and try to launch NetDirect again.
Server Error: please retry or contact Administrator	If invalid response received from the server	Try to reconnect again.
SPO Client can't run from outside/unpluged USB drive	SPO Client runs from Hard Disk	Run SPO Client from USB Disk
SPO Client can not run from Virtual Device.	SPO Client tries to launch from virtual drive	Start SPO Client from non virtual drive

Manual configuration of the log-level

This configuration can be done only for the Generic USB device and U3P device and not for CD ROM. Edit the configuration file-config.ini from Config folder located in the default SPO client folder. Under General option look for loglevel. Change the value to '2' which means 'info'. This value logs all the information from the client. It can also be accessed from the SPO client under tools/preferences. The SPO client must be connected to a AVG server to access the log from the SPO client interface.

Troubleshooting server for SPO

Verify the SPO user logged in by `/info/users` command from CLI. Also trace command (`/maint/starttrace usb`) helps to troubleshoot the communication between the server and the client.

Troubleshooting Delayed Write Failed issue

When the SPO is running, and you abruptly pull out the USB drive, Windows can generate a "Delayed Write Failed" error, and cause data loss. Perform one of these two action to avoid this error:

- Use the Unplug or Eject Hardware icon in the notification area to unplug the USB.
- Set the USB device properties to Optimize for quick removal.

Activating and using Ceedo log utility

Perform the following procedure to activate and use the Ceedo log utility.

Procedure steps

1. Open the CeedoLogControl.
2. Click **Run** to download the CeedoLogControl.exe file. A CeedoLog Control dialog box appears.
3. Click **Activate** to activate the Ceedo Log Control.
4. Run Ceedo, and then reproduce the error that you want to resolve.

   If reproduced, click **Deactivate** to stop the data recording of the Ceedo Log Control.
5. After you deactivate the Ceedo Log Control, open `%temp%\CeedoPersonalLogs\CeedoLogs\` to view the log files.
6. Archive the Ceedo log files, and then send the archived folder to Avaya.

   This utility configures the value of the `HKEY_CURRENT_USER\Software\Ceedo\CeedoLog` registry key that controls the log. The configuration details of this registry key are as follows:

Key	HKEY_CURRENT_USER\Software\Ceedo\CeedoLog
Value Name	UseLog
Value Type	Dword
Value	1 or 0

Troubleshoot cluster joining issues

This section explains how to troubleshoot issues related to clusters.

Joining an AVG to an existing cluster in the AVG Release 8.0

Perform the following procedure to troubleshoot cluster joining issue in the AVG Release 8.0.

Procedure steps

1. Enter this command to check whether the Host-based IP pool feature is enabled for a VPN in the cluster setup.

   ```
   /cfg/vpn #/hostippool
   ```

2. If enabled, enter this command to disable the Host-based IP pool feature for all the VPNs in the cluster.

   ```
   /cfg/vpn #/hostippool false
   ```

3. Join the AVG host to the cluster.
4. Enter this command to reenable the Host-based IP pool feature.

   ```
   /cfg/vpn #/hostippool true
   ```

5. Apply the configuration changes.

   A prompt appears asking you to configure the IP pool for the new host that is joined to the cluster automatically.

Join an AVG to an existing cluster

If you cannot join an AVG to a cluster, ensure that there is not a fault in the hardware encryption card. If the encryption card is not functioning properly, joining password cannot be matched to existing password. Replace the hardware.

Troubleshoot L2TP/IPsec issues

This section explains how to resolve issues related to L2TP/IPSec.

Troubleshooting user logon failure issue

Perform the following procedure to rectify the user logon failure issue.

Procedure steps

1. Enter this command to enable iketrace to funcentryexit.

```
/maint/debug/iketrace funcentryexit
```

2. Log on as the root user.
3. Enter this command to enable ikepacket dump.

   ```
   debugutil IKE SetPacketDump 1
   ```

4. Enable the trace for ike, ipsec, aaa, and l2tp.

For further debugging the issue, you can enable the client side IPSec log.

If the problem is with the L2TP/IPsec VPN connection, check the IPsec logs on your Windows workstation. The connection problems include troublesome firewalls, broken NAT devices, and IPsec authentication problems.

Enabling IPSec (IKE) logging

Perform the following procedure to enable IPsec (IKE) logging for more detailed log.

Procedure steps

1. Start the registry editor, and locate the following subkey with the administrator privileges:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ikeext
   \Parameters\EnableLogging
   ```

2. Set the **DWORD** value of **EnableLogging** to `1`.
3. Click **Start**, and then choose **Control panel** , **System and Maintenance**.

   OR

   Click **Start**, and then choose **Administrative Tools** , **Services**.
4. Select the **IKE and AuthIP IPSec Keying Modules (IKEEXT)** service.
5. Stop the service, and then start this service.

   Important:
   Do not use the Restart option to start the service again; restart does not have the same effect.

Alternatively, you can use the following procedure.

Procedure steps

1. At the DOS prompt, run the following commands as the administrator:

   ```
   NET STOP IKEEXT NET START IKEEXT
   ```

2. Initiate the L2TP/IPsec VPN connection that you want to troubleshoot, and then disconnect the connection if it is not yet terminated.
3. Stop the IKEEXT service.

Windows Vista creates an Event Trace Log file in the `%SystemRoot%\System32\Ikeext.etl`. This ETL file is a binary file.

4. Convert the Ikeext.etl file into a readable output using the tracefmt.exe file.

   This tool is included in the Windows XP Support Tools pack.

5. To convert this file into a readable output, open Windows XP Service Pack 2 Support Tools.

6. Run the tracefmt.exe file.

   Windows Vista can report a compatibility problem; ignore the warning. Some of the programs in the Windows XP Service Pack 2 Support Tools are probably not compatible.

   Important:
   Do not install any tool other than tracefmt.exe.

   Alternatively, you can install the Support Tools pack on a Windows XP SP2 machine, and then copy the files tracefmt.exe and traceprt.dll into a directory on your Windows Vista machine.

7. Run this command with administrator privileges:

   ```
   tracefmt.exe %SystemRoot%\System32\Ikeext.etl -tmf
   %SystemRoot%\System32\wfp.tmf -o %TEMP%\wfpdiag.txt
   ```

   The system creates wfpdiag.txt file. This file is similar to the oakley.log on Windows 2000/XP. You can view this file with `write.exe %TEMP%\wfpdiag.txt`.

8. Start the IKEEXT service again.

Troubleshoot Web Rewrite issue

This section explains how to troubleshoot issues related to Web Rewrite. The following issues can occur:

- unsuccessful page loading with script errors, missing page content, or page layout issues
- Simpleproxy crash message in the log file
- high CPU utilization

Troubleshooting unsuccessful page loading issues

This section explains the steps to troubleshoot the issues related to unsuccessful page loading. The possible issues are script errors in page loading, missing page content, or incorrect page layout. These issues occur because of the incompatibility of the AVG parser with the Web document.

AVG supports various client-based solutions to supplement the Web Rewrite service. If a page is causing an issue with the AVG portal, the administrator can provide the following client-based solutions to the end user while issues are being investigated.

- Portforwarder
- Net Direct
- L2TP/IPSec client
- Contivity IPSec client

Perform the following procedure to troubleshoot unsuccessful page loading issue.

Procedure steps

1. Check the application compatibility matrix.
2. Check the latest release notes.
3. Enable the following command to locate the problematic page.

   ```
   traflog
   ```

4. Use the HTTP Analyzer tool for packet capture. If the HTTP Analyzer is not available, use the TCPDUMP for packet capture.
5. Collect the packet capture with and without AVG.
6. Compare the packet capture to identify the problem.
7. Implement a client-based solution as a work around.

Troubleshooting Simpleproxy crash issues

Perform the following procedure to troubleshoot the issues related to a Simpleproxy crash. These issue can occur due to the following reasons:

- incompatibility of AVG parser with Web document
- SSL handshake failure
- Simpleproxy overload

Perform the following procedure to resolve this issue.

Procedure steps

1. Enable the following command to log the HTTP request.

   ```
   traflog
   ```

2. Check the newly added or upgraded intranet applications.
3. Check the application compatibility matrix.
4. Check the latest release notes.

5. Enable the following command to generate detailed debug information.

   ```
   proxydebug
   ```

6. Enable the following command to dump the core file.

   ```
   proxycore
   ```

7. Run the following command to collect the AVG server log.

   ```
   /maint/dumplog
   ```

Troubleshooting high CPU utilization issues

This section explains the steps to troubleshoot the issue related to high CPU utilization. These issues can occur due to the following reasons:

- incompatibility of AVG parser with Web document, especially with Javascript
- bad client certificate
- debug message enabled

To troubleshoot this issue, first check the latest release notes to ensure that this is not an OpenSSL issue. If the issue is not an OpenSSL issue, ensure that the **`proxybug`** is enabled. If so, disable it.

If the problem persists, perform the following procedure.

Procedure steps

1. Check for the newly added or upgraded intranet applications.
2. Check the application compatibility matrix.
3. Check the latest release notes.
4. Run the following command to check the number of session.

   ```
   /info/licenses
   ```

Chapter 6: Troubleshooting authentication tasks

This chapter provides information to troubleshoot authentication issues. For information about the Avaya SSL VPN commands or concepts go to http://www.avaya.com

Navigation

Troubleshooting RADIUS authentication

The IAS checks the Active Directory to validate a username/password when a RADIUS authentication request arrives from the SSL VPN gateway. Further, it returns an attribute in the RADIUS authentication response that will map the user to the correct group/groups in the SSL VPN configuration. The user can use the network user name, as defined in Active Directory, when authenticating.

Important:

The configuration attributes given in this section are just examples. The attributes that you need to specify for configuration can be different than this.

Troubleshooting RADIUS authentication navigation

Configuring RADIUS settings

Perform the following procedure to configure the different RADIUS settings.

Procedure steps

1. Enter the following command to add a RADIUS server name.

   ```
   /cfg/vpn #/aaa/auth 2/type radius/name "radius.avaya.se"
   ```

2. Enter the following command to add multiple servers.

   ```
   /cfg/vpn #/aaa/auth 2/radius/servers/add 172.25.3.50 1812
   secret
   ```

3. Enter the following command to add the authentication order of the SSL VPN Gateway.

   ```
   /cfg/vpn #/aaa/authorder 2,1
   ```

Variable definitions

Use the data in the following table to help you enable configure the parameters in this command.

Variable	Definition
authorder	Specifies the auth order of the SSL VPN gateway to authenticate a user. **Important:** With this option the SSL VPN gateway will first try the RADIUS server, in case the user is not authenticated or the server timeout limit is reached, the SSL VPN gateway will check the Local user database.
name	Specifies the name of the RADIUS sever. **Important:** The name option is only internal in the box/cluster it will not show up in the Login Service drop-down box as in previous version.
secret	Specifies the shared RADIUS secret used in the communication between the RADIUS client and server.

Integrating authentication service

This section explains the steps to integrate various authentication services. The first time you start the Internet Authentication Service manager you will have to register the IAS in the Active Directory to allow the integration to happen.

Integrating authentication service navigation

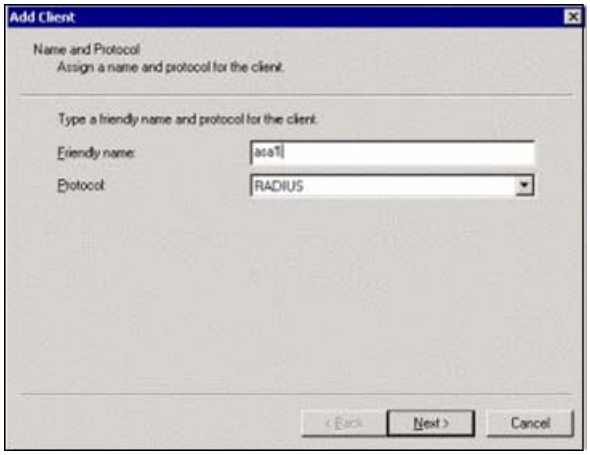
Adding a new RADIUS client

Perform the following procedure to add a new RADIUS client to the server.

Procedure steps

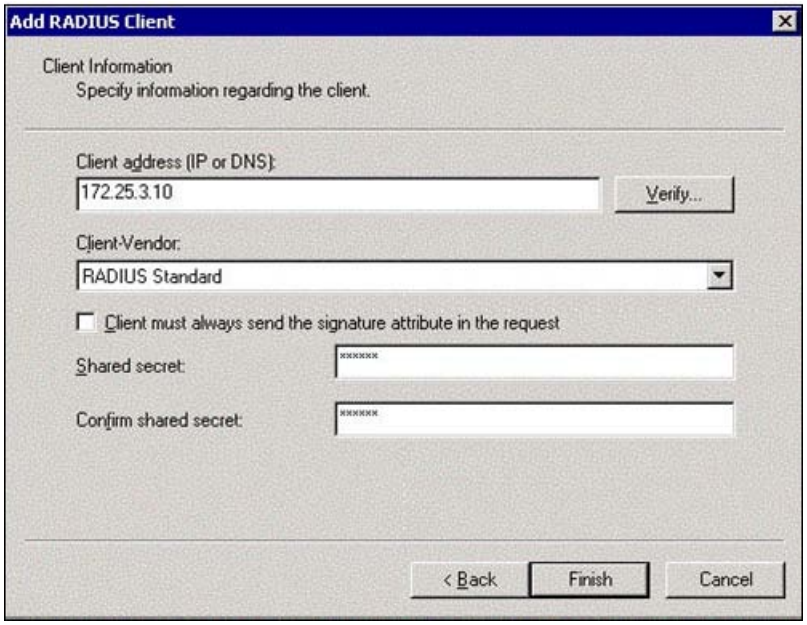
1. From the **Action** menu bar, select **Register Service in Active Directory**.
2. In the tree view, right click on **Clients** and select **New Client**.

   Add client dialog box appears.



3. Enter the RADIUS client friendly name.
4. Click **Next** to continue.

   Add RADIUS client dialog box appears.



5. Enter the IP address or host name for the RADIUS client.
6. Add and confirm the shared secret.
7. Click **Finish**.

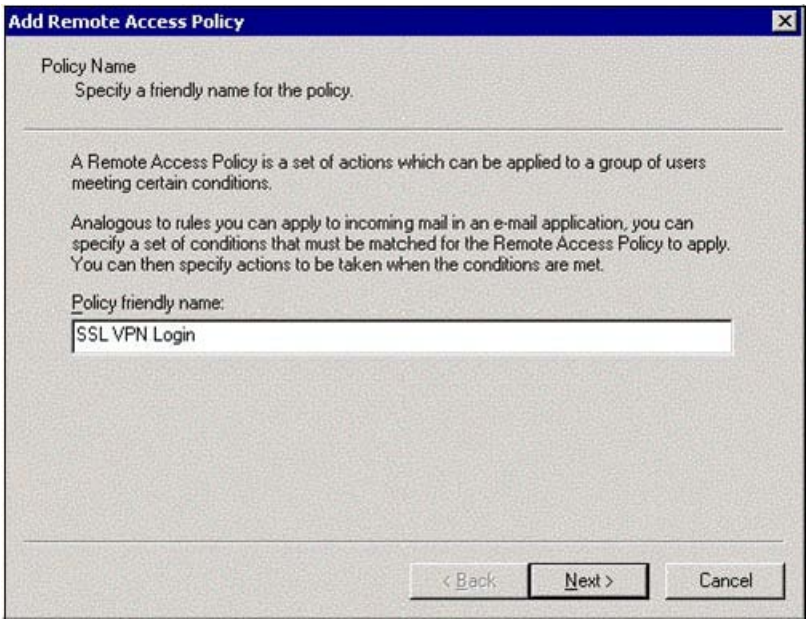
Configuring new Remote Access Policy

This section shows the example for a basic set up with only one group available in the SSL VPN gateway. The Remote Access Policy will set the criteria for how the RADIUS authentication request will be processed and it will also perform the user to group/groups mapping.

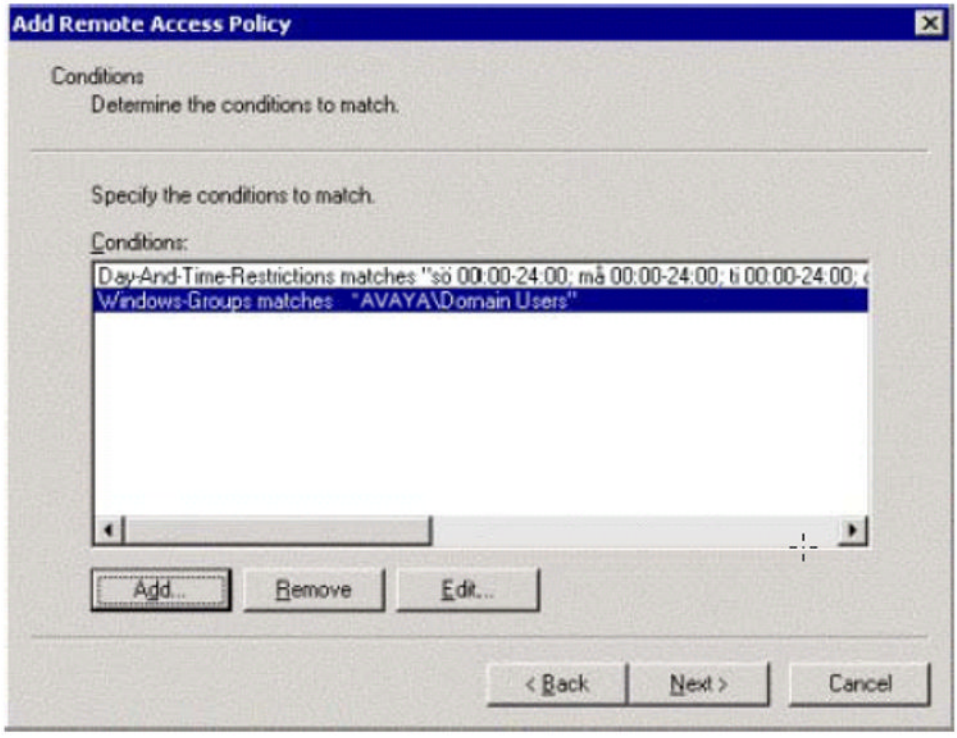
Procedure steps

1. In the tree view, right click **Remote Access Policies** and select **New Remote Access Policy**.

   Add Remote Access Policy dialog box appears.



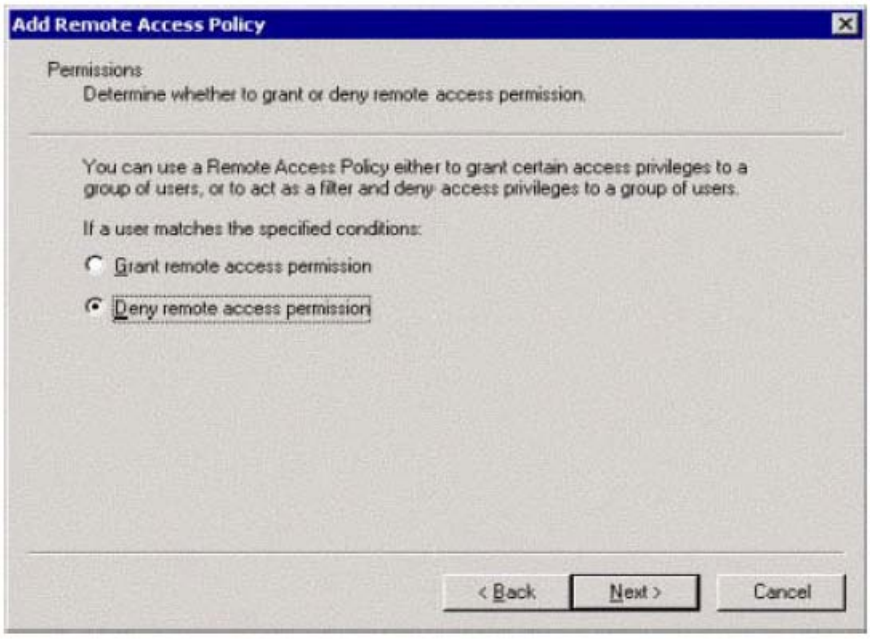
2. Enter the Remote Access Policy friendly name.
3. Click **Next** to continue.



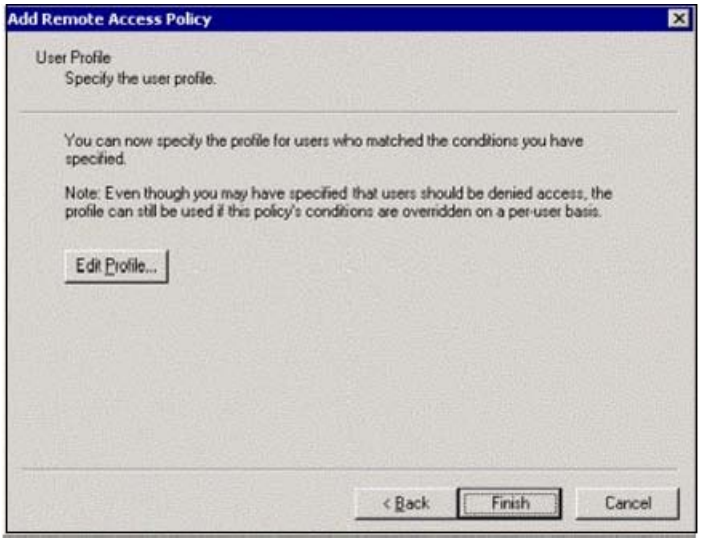
4. Select the conditions for which this Remote Access Policy will match.

   The conditions can include Day and Time restrictions, Windows groups a user belongs to, from which IP address the RADIUS authentication requests arrives, and so on.

5. Click **Next** to continue.
6. Select **Deny remote access permission**.

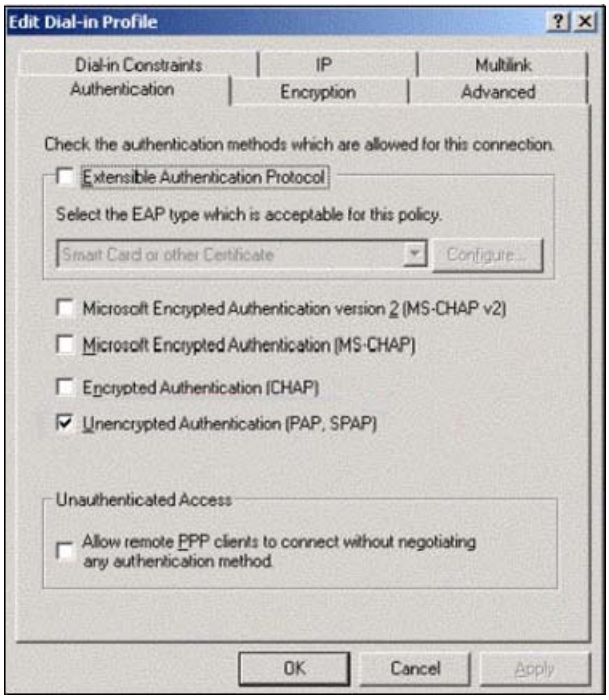


7. Click **Next** to continue.



8. Click **Edit Profile**.

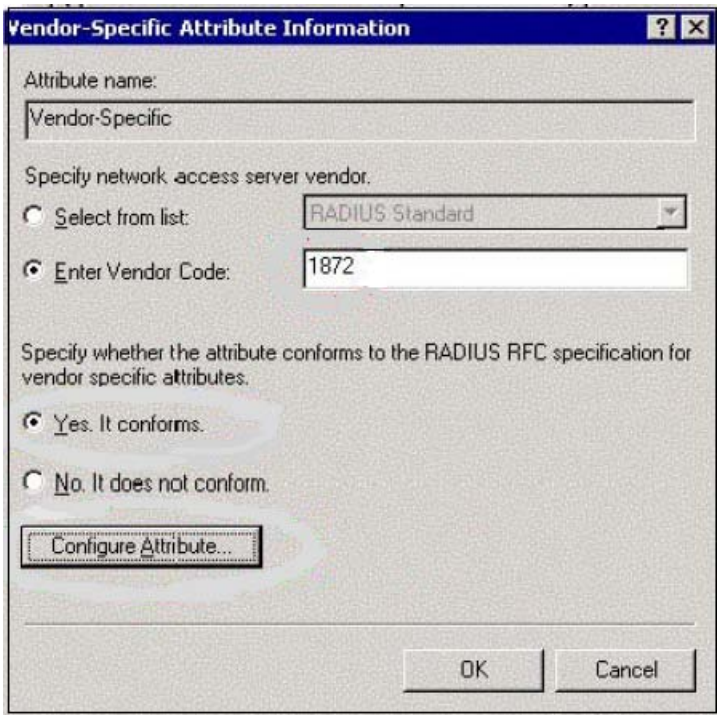
   Edit Dial-in Profile form appears.



9. Under **Authentication** tab, check the option **Unencrypted Authentication (PAP, SPAP)**.
10. Click on **Advanced** tab to continue.
11. Specify the RADIUS attributes that is returned to a RADIUS client.
12. Click **Remove** twice to default values that are not needed.
13. Click **Add** and select the Vendor-Specific attribute.

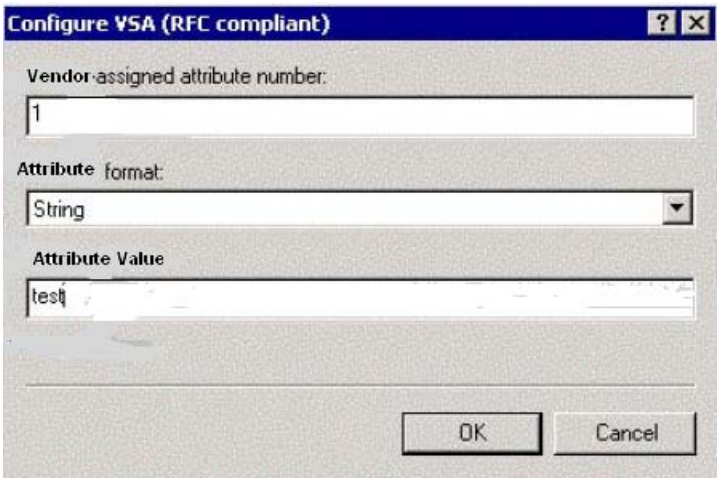
    Multivalued Attribute Information form appears.
14. Click **Add** to continue.

    Vendor-Specific Attribute Information form is displayed.



15. Configure the Alteon specific RADIUS vendor id , for example 1872.
16. Select **Yes. It conforms**.
17. Click **Configure Attribute** to continue.

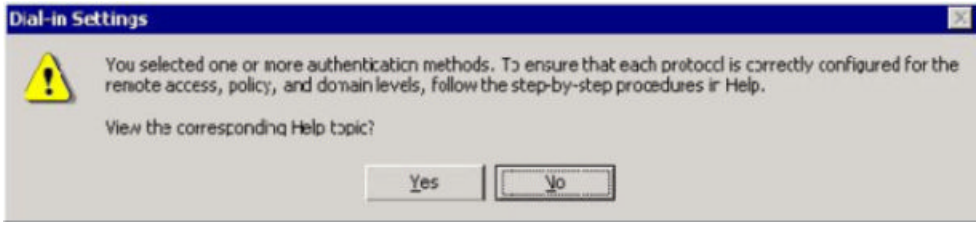
    Configure VSA RFA Compliant form is displayed.



18. Set the Vendor-assigned attribute number to 1.
19. Specify the name of the SSL VPN gateway group in the Attribute value.
20. Click **OK** twice to return to the main Vendor-Specific attribute screen.
21. Click **OK** then **Close** to get back to Dial-in Profile screen.

22. Click **OK** in the Dial-in Profile screen to get back to the Remote Access Policy wizard.

    The Dial-in Settings warning screen appears.



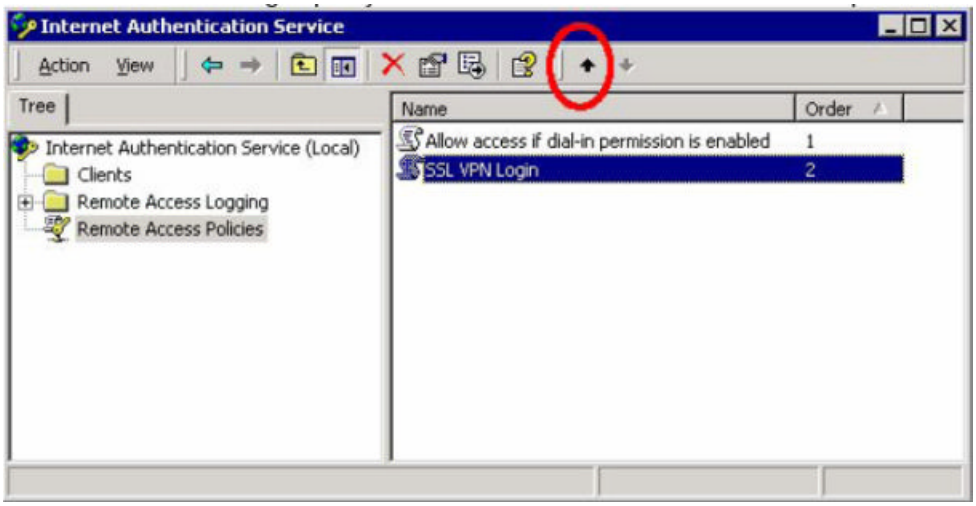
23. Click **No** to continue.
24. Click **Finish** in Remote Access Policy Wizard to finalize Remote Access Policy configuration.

Arranging the order of the Remote Access Policies

Perform the following procedure to arrange the order of the remote access policies.

Procedure steps

In Internet Authentication Service wizard, select SSL VPN Login policy and click on Up-arrow in the menu to move it up in the list.

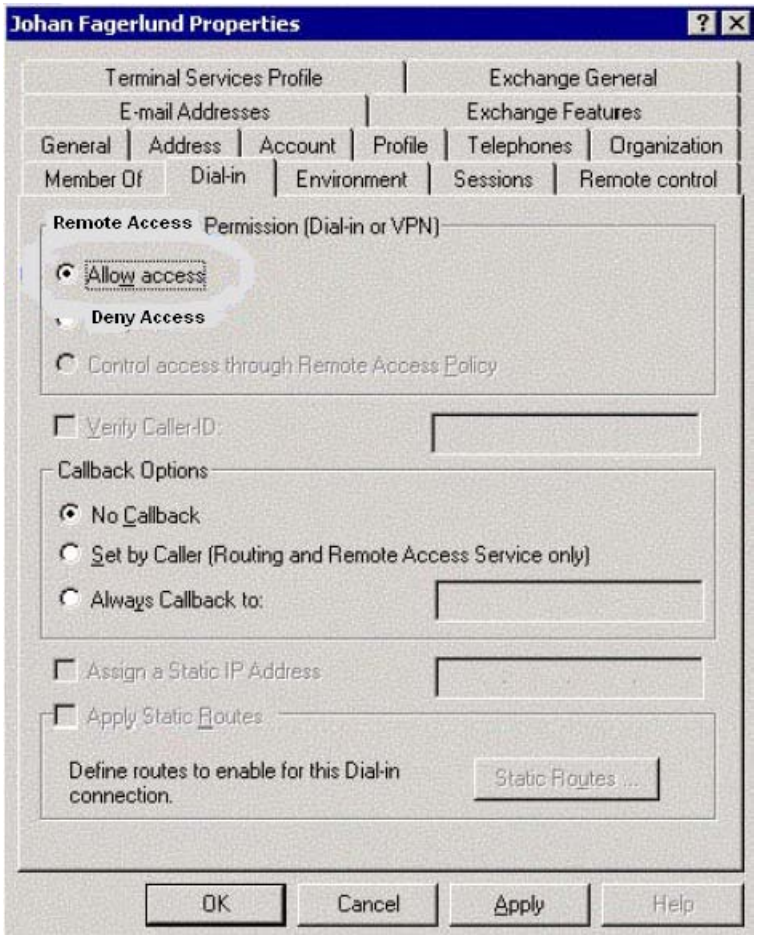


Adding new users and changing existing users

This section explains how to add a new user or change an existing user. These users must meet one of the Remote Access Policies conditions belonging to the correct Windows group.

Procedure steps

1. In the User name Properties screen, select **Member Of** to check if the user meets the Remote Access Policies conditions.
2. Click **Dial-in**.



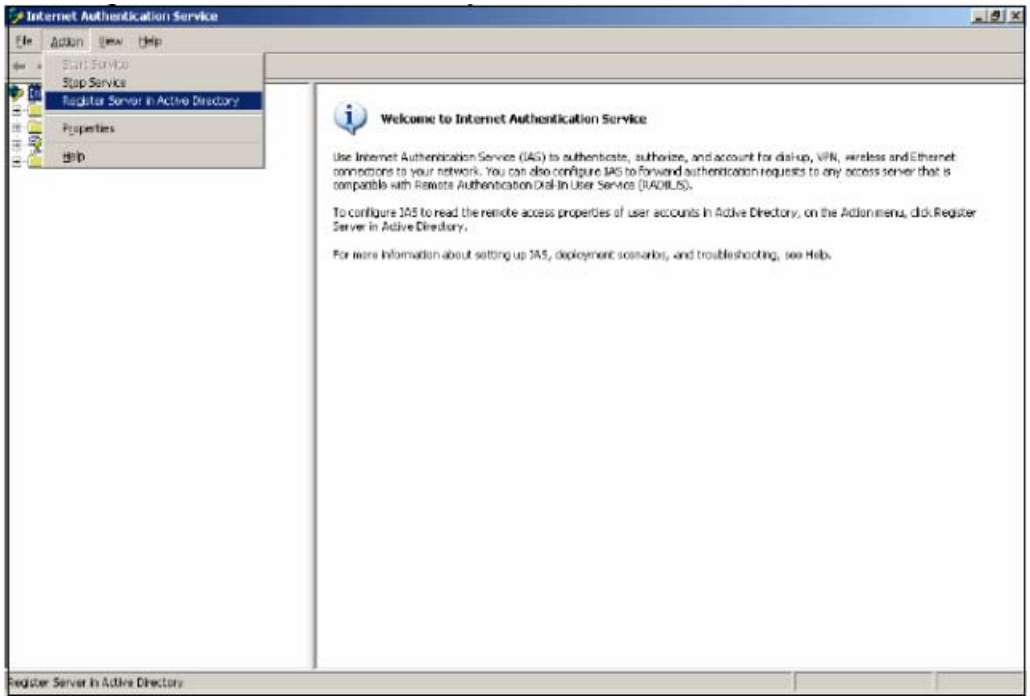
3. Select **Allow Access**.
4. Click **OK** or **Apply** to active the user settings.

Registering the IAS in the Active Directory

Perform the following procedure to register the IAS in the Active Directory to allow the integration to happen.

Procedure steps

From **Action** menu, select **Register Server in Active Directory**.

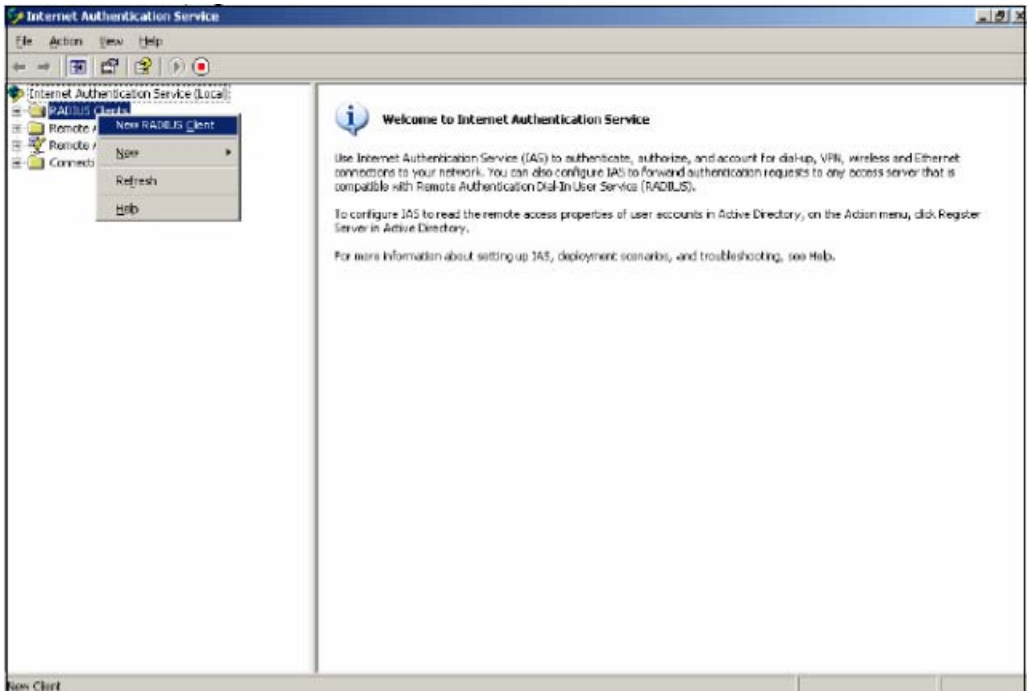


Adding a new RADIUS client that uses the IAS

Perform the following procedure to add a new RADIUS client that uses the IAS.

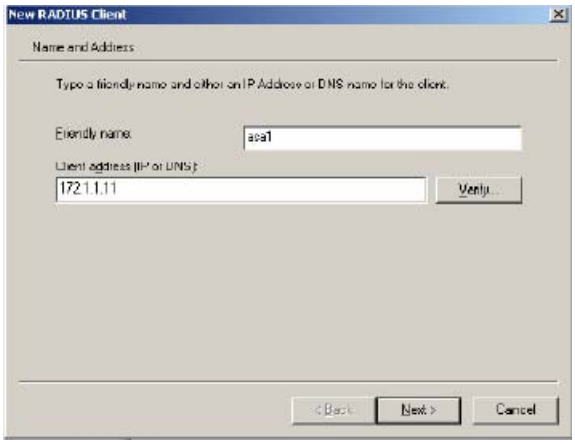
Procedure steps

1. In the tree view of Internet Service Authentication screen, select the client.

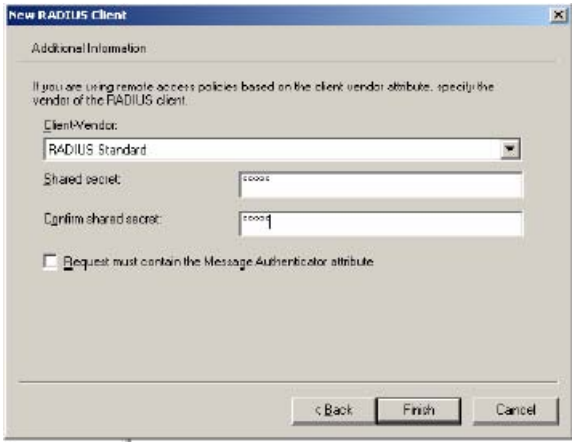


2. Right click on the client and select **New RADIUS Client**.

   Add New RADIUS Client form appears.



3. Specify the name of the RADIUS client with a friendly name.
4. Specify the IP address or host name for the RADIUS client.
5. Click **Next** to continue.
6. Add and confirm the shared secret.



7. Click **Finish**.

Troubleshooting LDAP authentication with Active Directory

LDAP is used to communicate with a directory server. If users do not want to use the full name of the Windows Group, then they need to find another attribute in the AD schema that they can use as the group attribute or use the short group format feature

```
/cfg/vpn #/aaa/auth #/ldap/enashortgr.
```

Troubleshooting LDAP authentication with Active Directory navigation

- Troubleshooting LDAP authentication issues on page 57
- Adding an SSL VPN gateway user into the Active Directory on page 58
- Configuring the LDAP Attributes on page 60

Troubleshooting LDAP authentication issues

Perform the following procedure to set isdbindn and isdbin password, if they are not correctly set.

Procedure steps

1. Enter the following command to set the LDAP bind DN.

   ```
   /cfg/vpn #/aaa/auth #/ldap/isdbinddn
   ```

2. Enter the following command to set the LDAP bind password.

```
/cfg/vpn #/aaa/auth #/ldap/isdbindpasswd
```

Important:
Use ldap browser to verify search base and attributes.

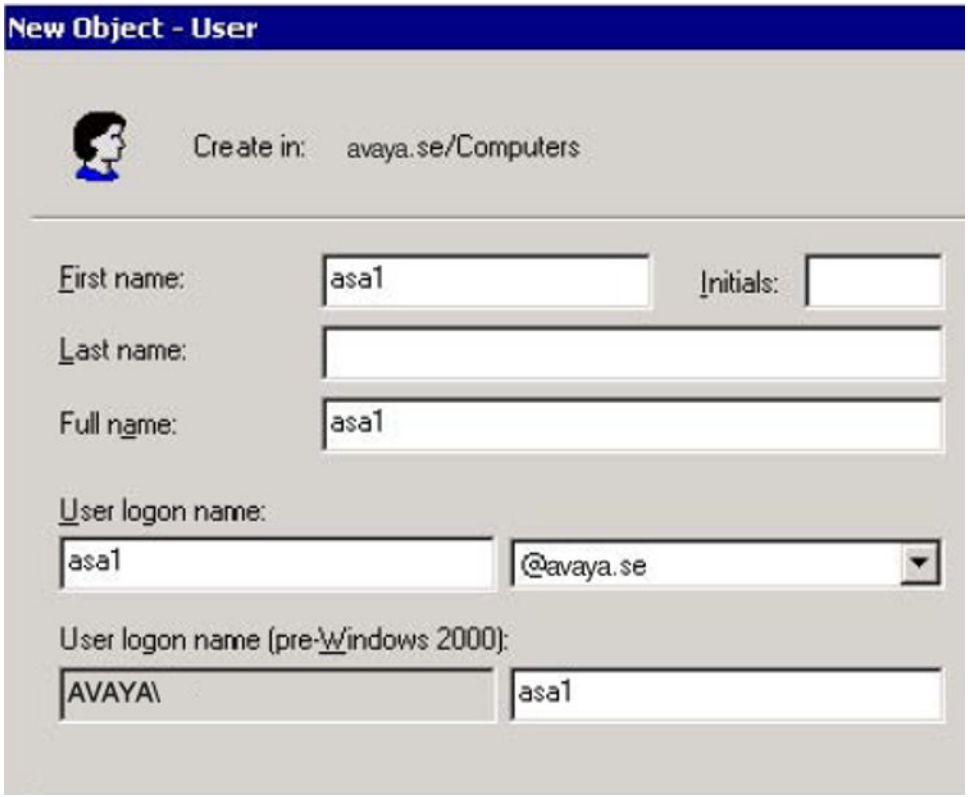
Adding an SSL VPN gateway user into the Active Directory

Perform the following procedure to add an SSL VPN gateway user into AD.

Procedure steps

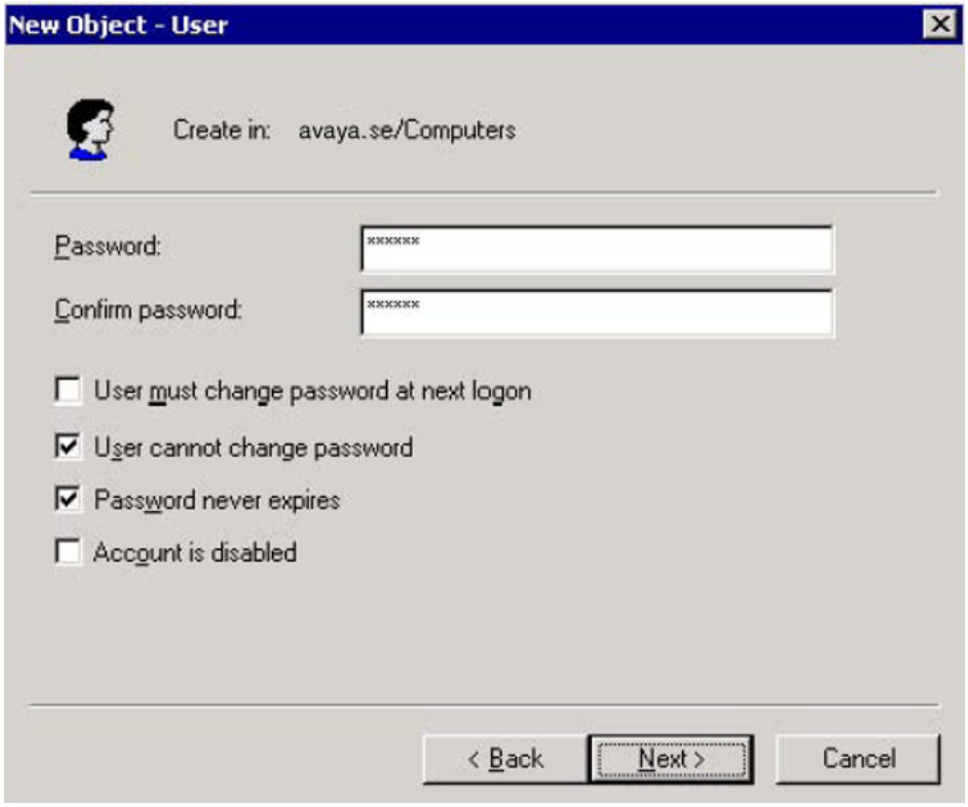
1. In the **Active Directory Users and Computers** screen, select the branch from the tree view.
2. Click on **Create a new user** icon in the menu, to create a new user.

   New Object –User dialog box appears.



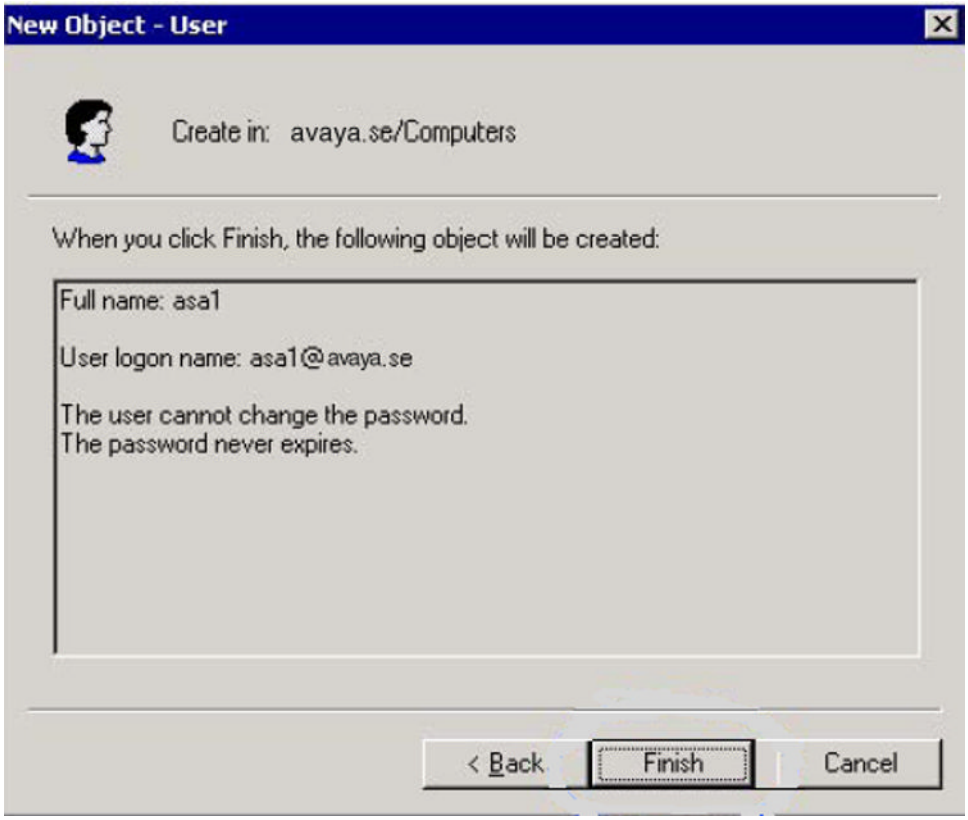
3. Specify the **First name** and **User Logon name**.

   For example, first name can be asa1 and userlogon can be asa1@avaya.com
4. Click **Next** to go to the next page.



5. Specify the password that is use to authenticate SSL VPN gateway.

   For example, secret. You can also add some additional password restriction.
6. Click **Next** to continue.



7. Click **Finish** to complete adding a user.

Configuring the LDAP Attributes

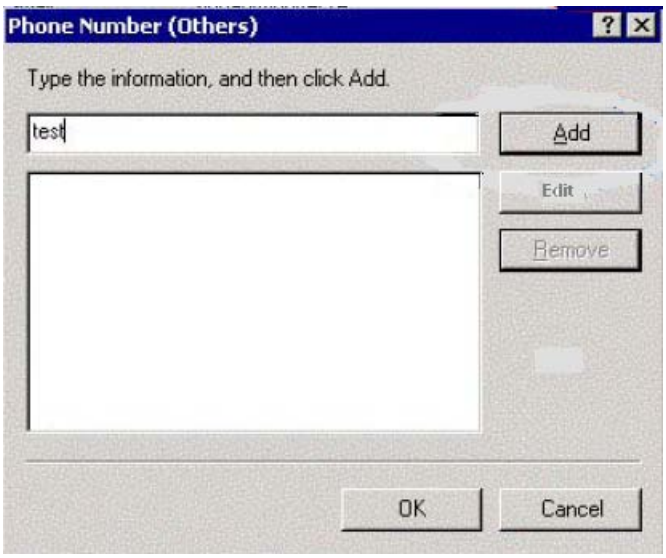
Perform the following procedure to configure LDAP Attributes.

Procedure steps

1. In the User name Properties screen, click **General** tab.

2. Click **Other** adjacent to the field Telephone number.

   Phone Number (Others) form is displayed.



3. Enter the name of the SSL VPN gateway groups the user belongs to and click **Add**.
4. Click **OK** to activate the changes.

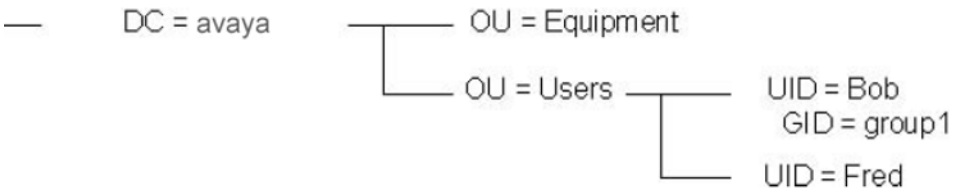
   In the directory tree the attributes appears and are use-able by the SSL VPN gateway when querying for the group attribute

Configuring LDAPs authentication with Active Directory

LDAP is used to communicate with a directory server. There are many directory servers available in the market that uses LDAP for communication, like Novell NDS or e-Directory, Sun ONE Directory Server, OpenLDAP, and also Microsoft Active Directory.

A directory server is a structured tree where not only user information but other related information can be stored. Different branches build up each directory tree and on each branch there is one or multiple attributes, each attribute can have one or multiple values. Each branch in the directory tree has it's own unique identifier or distinguished name. The distinguished name is built from the root including all the branches.

When you configure the SSL VPN gateway for LDAP authentication one of the key parameter to configure is the searchbase. The searchbase instructs the SSL VPN gateway where, in the directory tree, it would start searching for the user attribute. The user attribute or userattr indicates which attribute contains the user name. Once the searchbase is configured, you need to configure the group attribute or groupattr, which indicates that the group mapping in the SSL VPN configuration. With the directory tree looking the way it does above the searchbase would be "OU=Users,DC=Avaya" the userattr would be "UID" and finally the groupattr would be "GID".



Procedure steps

1. Configure LDAP as shown in the section Adding an SSL VPN gateway user into the Active Directory on page 58
2. Enable LDAPS support on the SSL-VPN.

   `/cfg/vpn #/aaa/auth #/ldap/enaldaps true`
3. Add LDAPS server with port 636.

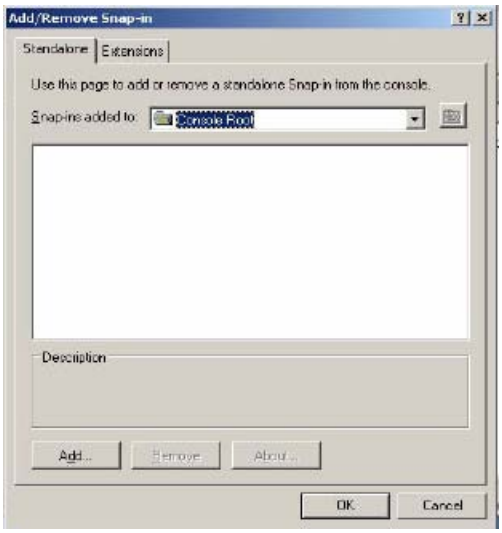
   `/cfg/vpn #/aaa/auth #/ldap/servername/add` IP Address to add: 172.1.1.200 Port (default is 389): 636
4. Click **Apply**.
5. Generate a test cert and export for use on the AD server.

   `/cfg/cert #`

   Important:
   The CN must match the FQDN of the actual AD server.
6. Click **Apply** to activate.

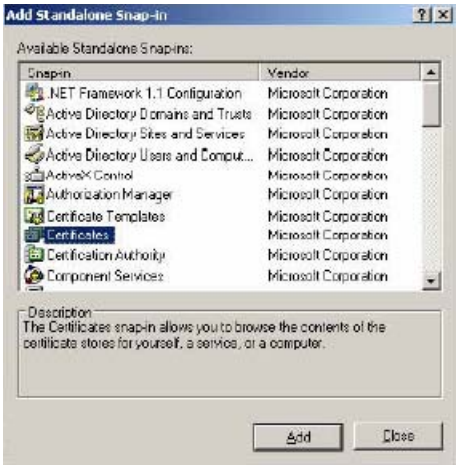
7. Login to AD server and open MMC.
8. Add certificate store snap-in for Local Computer.
9. In the Console wizard, under file menu, select **Add/Remove Snap-in**.

   Add/Remove Snap-in form appears.



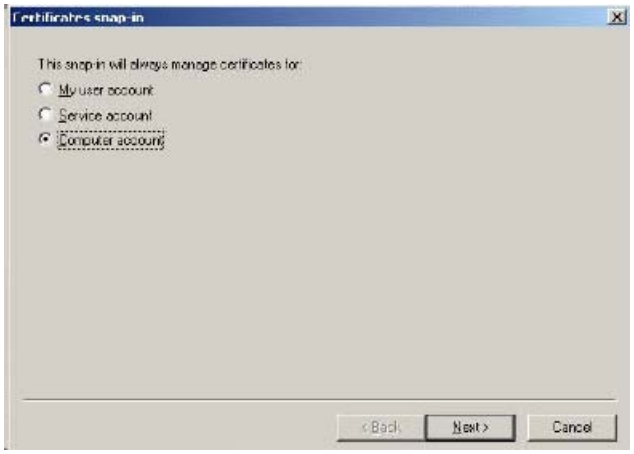
10. Click **Add**.

    Add Standalone Snap-in form appears.

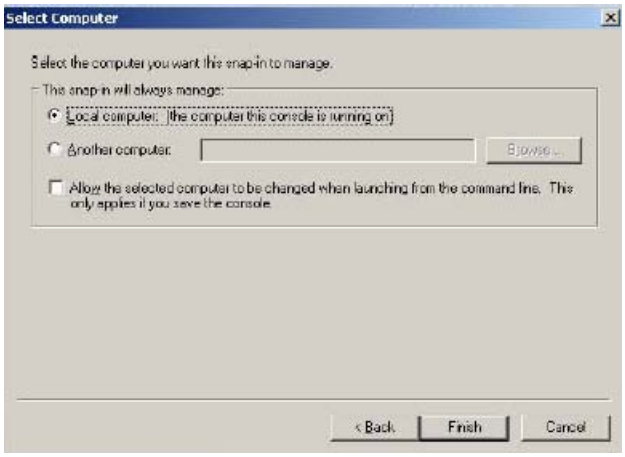


11. Select the available Standalone Snap-in and click **Add**.

    Certificate Snap-in form appears



12. Select **Computer Account**.
13. Click **Next** to continue.



14. Select the option **Local computer: the computer this console is running on**.
15. Click **Finish**.

    The certificate is now available in the Add/Remove Snap-in form.

Importing certificates

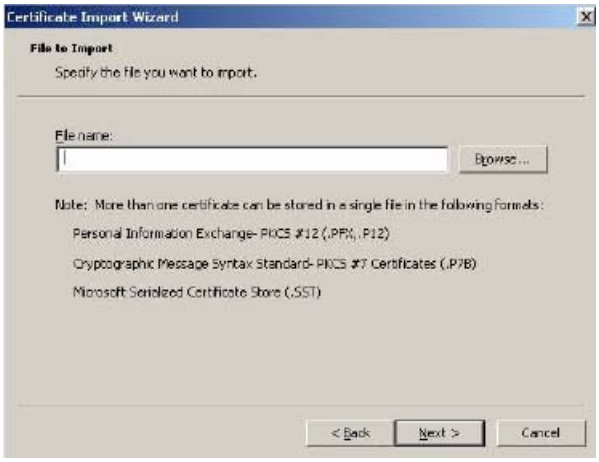
Perform the following procedure to import certificates under Local computers.

Procedure steps

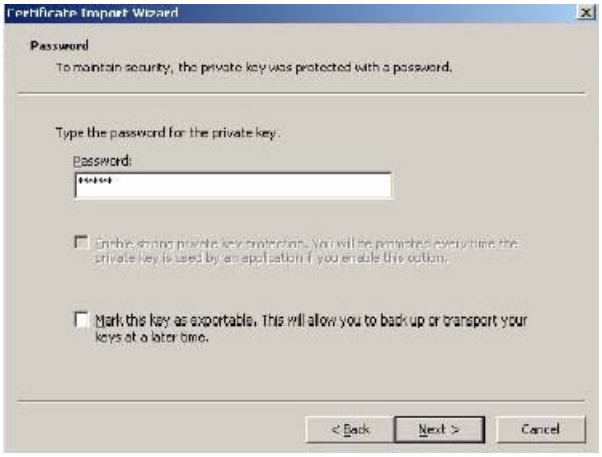
1. To import the certificate, select Import in **All Tasks** under **Action** menu.

   Certificate Import Wizard appears.

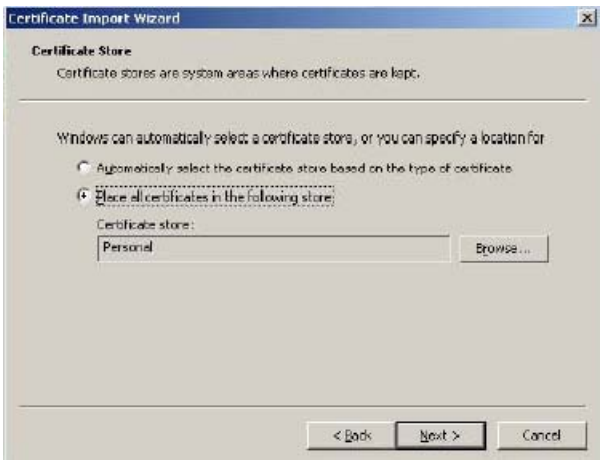
2. Click **Next**.



3. Browse for the file name and click **Next**.



4. Enter the password and click **Next**.



5. Select option **Place all certificates in the following store** and click **Next**.

6. Click **Finish** to complete the import of the certificate.
7. Import same certificate under **Local Computer -> Trusted Root Certification Authorities**.
8. Verify the Event Viewer shows the LDAP over SSL has started.
9. Verify LDAPS auth works correctly.

   If the authentication fails, check and verify that the CN is the AD servers FQDN.

Important:

You will also see a failure in the Event Viewer if the AD server is not configured correctly

Troubleshooting NTLM authentication with Primary Domain Controller

NTLM is a authentication protocol used by Windows clients to authenticate towards Windows Domain Controllers.

NTLM is supported in Windows 2000 for users with need for backwards compatibility. The SSL VPN gateway will authenticate users towards an NTLM Domain Controller natively, that is, addition software is not required on the Domain Controller.

Also the user to group/groups mapping is supported using NTLM. The SSL VPN gateway will query the Domain Controller for the Windows groups a user belongs to and map that to SSL VPN gateway group/groups.

Troubleshooting NTLM authentication with Primary Domain Controller navigation

- Creating the Windows group and add a user into that group on page 67
- Adding users to the new group on page 68

Creating the Windows group and add a user into that group

To allow the SSL VPN gateway to map a Windows user to the test group in the SSL VPN group you need to create a global Windows group with the same name.

Procedure steps

1. Start the Active Directory Users and Computer manager.
2. Click on the **Create new group** icon in the Active Directory Users and Computers screen.

   New Object-Group form appears.
3. Specify the group name.
4. Select **Security** in group type.
5. Click **Next** to continue.
6. Click **Finish** to create a group.

Adding users to the new group

Perform the following procedure to add users to a new group.

Procedure steps

1. Click **Member Of** tab in User name Properties screen.
2. Click **Add**.

   Select Groups form is displayed.
3. Select the group.
4. Click **Add**.
5. Click **OK** to finish the group selection.

   The user is now part of the correct group that will allow the SSL VPN gateway to map the user into the test group.
6. Click **OK** to save the user properties.

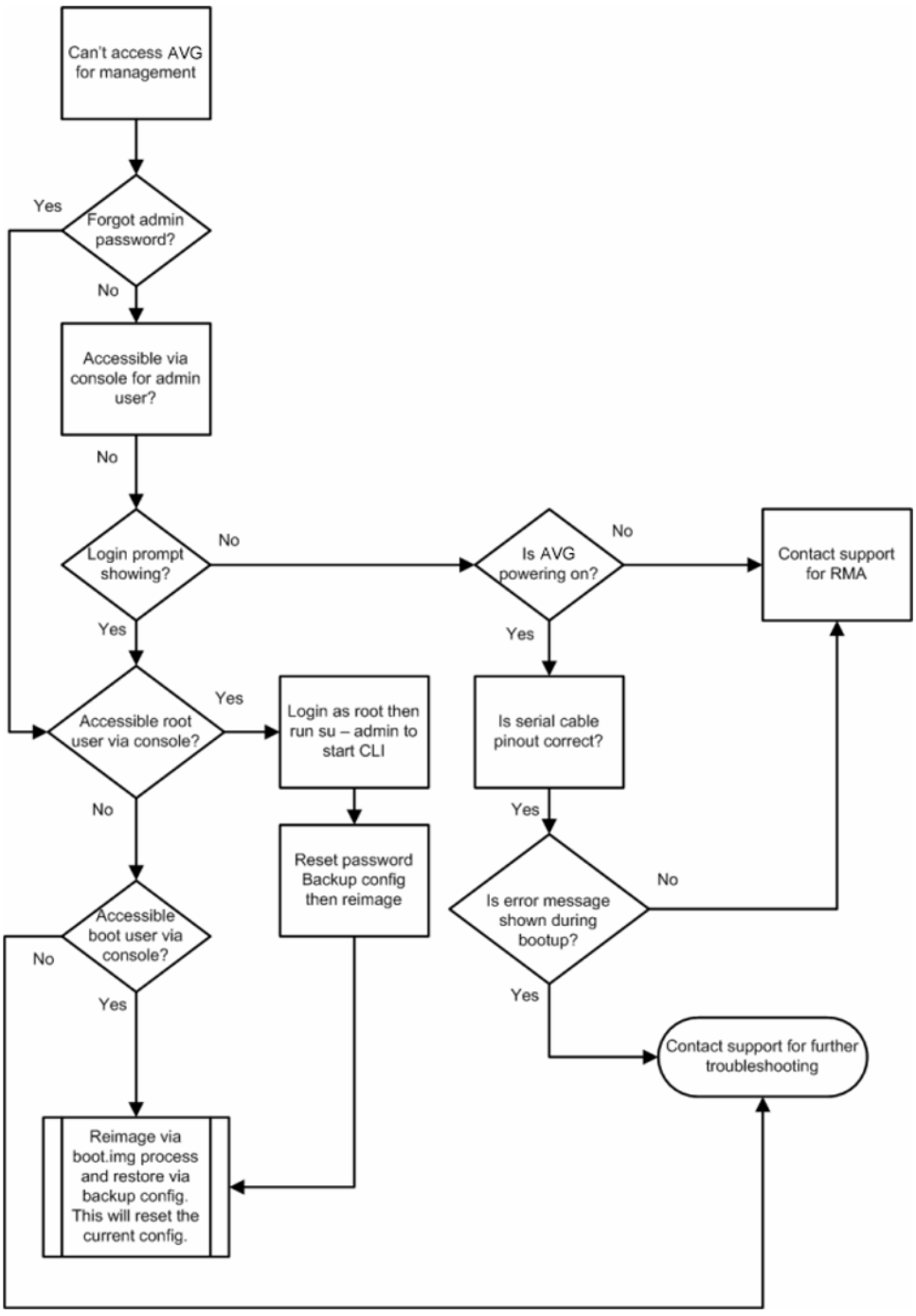
Chapter 7: Emergency Recovery Trees

This chapter provides the procedures to recover from field outages as quickly as possible.

This chapter includes the following topics:

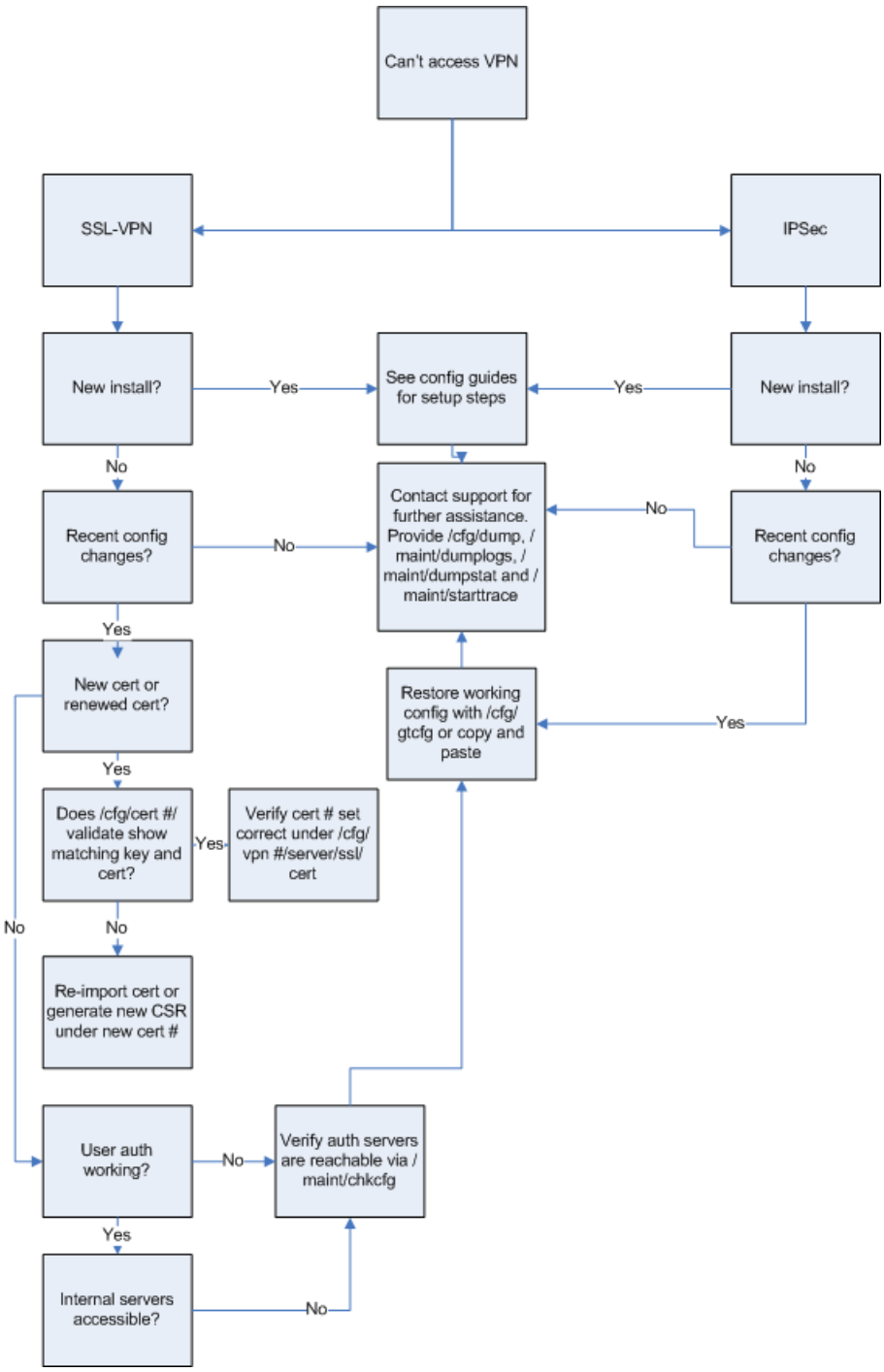
Cannot access AVG for management — recovery tree

This section details the flow diagram for the recovery tree — cannot access AVG for management.



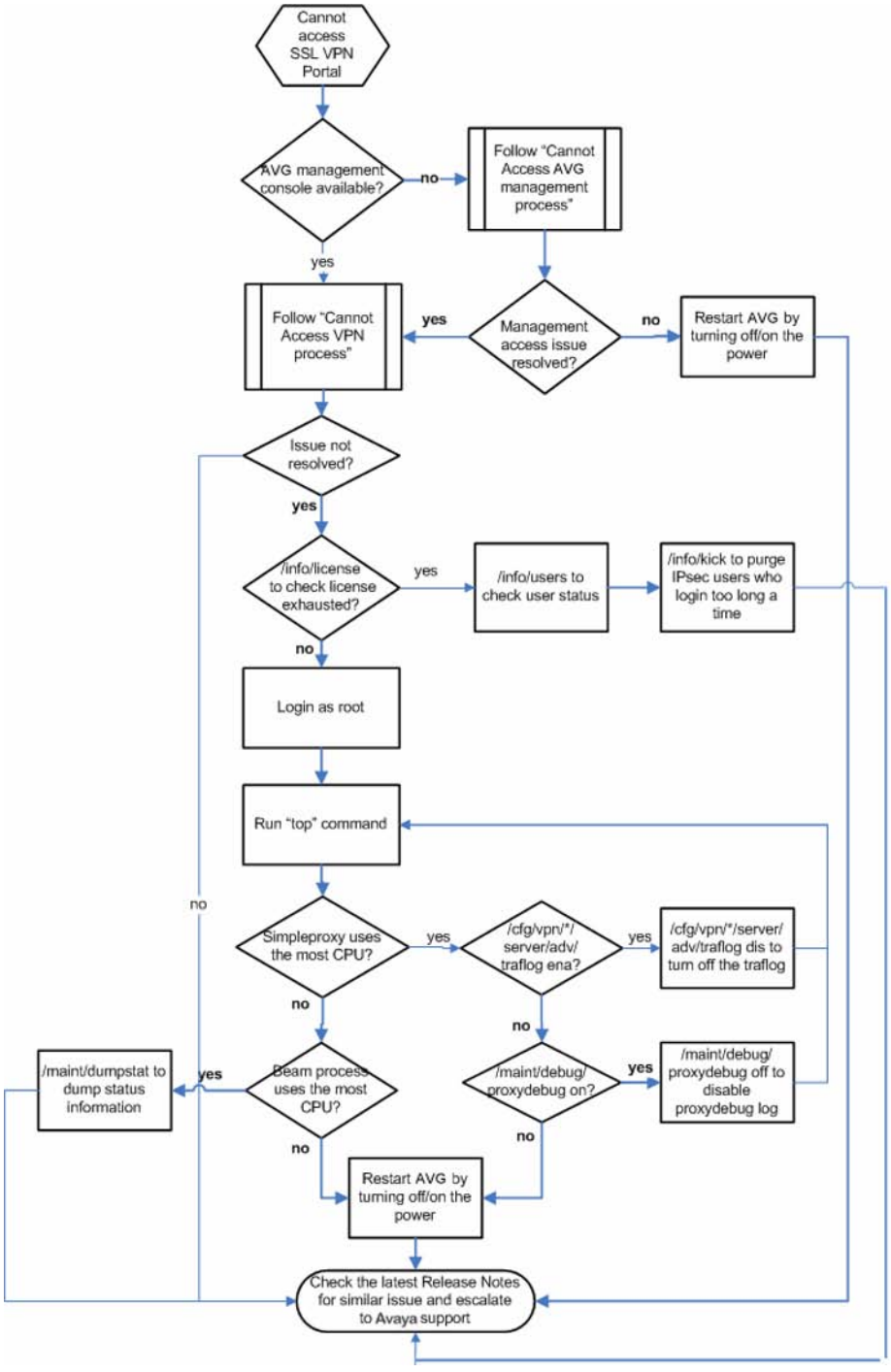
Cannot access VPN — recovery tree

This section details the flow diagram for the recovery tree — cannot access VPN.



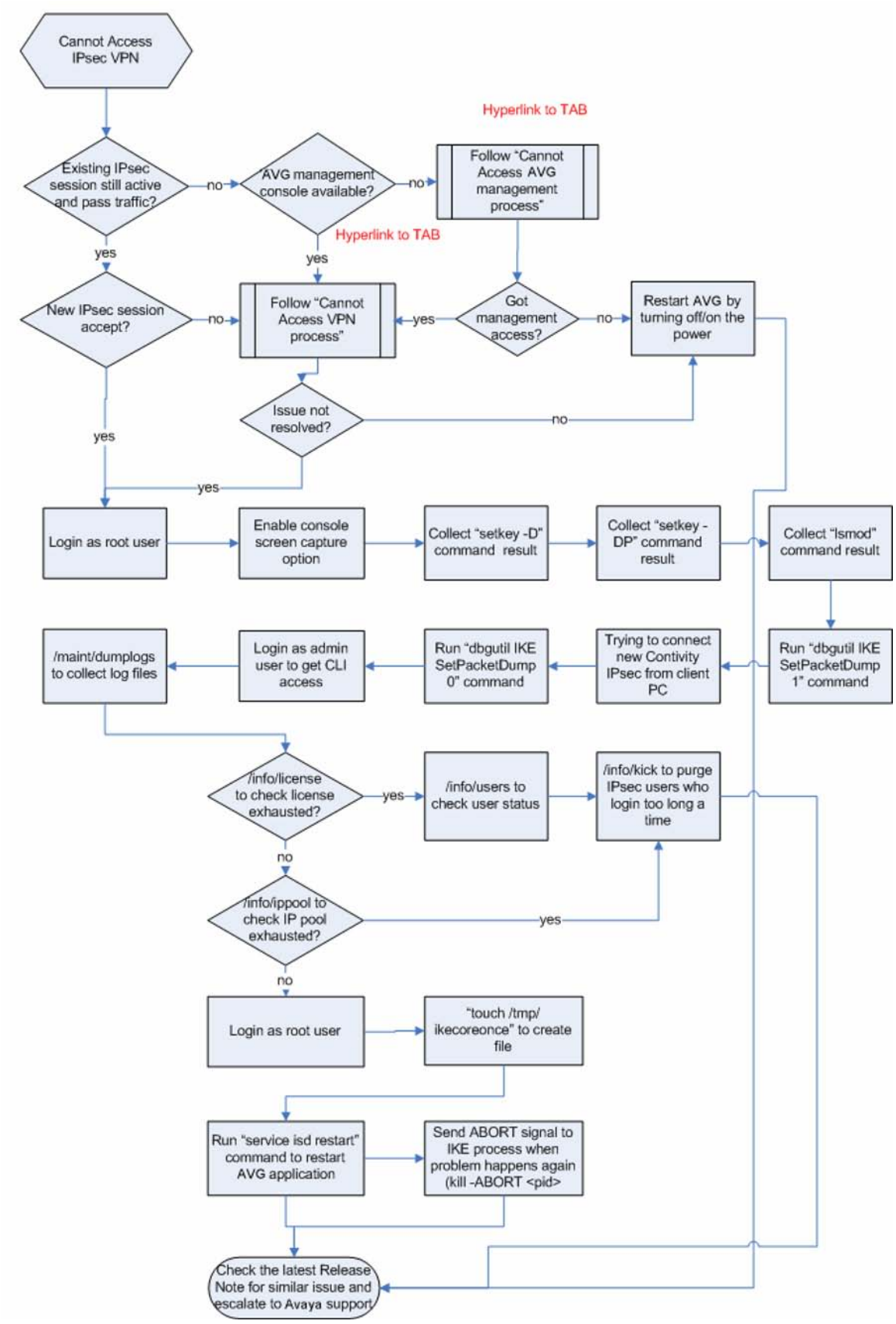
Cannot access SSL VPN Portal — recovery tree

This section details the flow diagram for the recovery tree — cannot access SSL VPN Portal.



Cannot access IPsec VPN — recovery tree

This section details the flow diagram for the recovery tree — cannot access IPsec VPN.


Cannot Access IPsec VPN
Existing IPsec session still active and pass traffic?
no
AVG management console available?
no
Hyperlink to TAB
Follow "Cannot Access AVG management process"
Hyperlink to TAB
yes
yes
New IPsec session accept?
no
Follow "Cannot Access VPN process"
yes
Got management access?
no
Restart AVG by turning off/on the power
Issue not resolved?
no
yes
yes
Login as root user
Enable console screen capture option
Collect "setkey -D" command result
Collect "setkey -DP" command result
Collect "lsmod" command result
/maint/dumplogs to collect log files
Login as admin user to get CLI access
Run "dbgutil IKE SetPacketDump 0" command
Trying to connect new Contivity IPsec from client PC
Run "dbgutil IKE SetPacketDump 1" command
/info/license to check license exhausted?
yes
/info/users to check user status
/info/kick to purge IPsec users who login too long a time
no
/info/ippool to check IP pool exhausted?
yes
no
Login as root user
"touch /tmp/ikecoreonce" to create file
Run "service isd restart" command to restart AVG application
Send ABORT signal to IKE process when problem happens again (kill -ABORT <pid>
Check the latest Release Note for similar issue and escalate to Avaya support

Reimage AVG — recovery tree

This section details the flow diagram for the recovery tree — reimage AVG.

Chapter 8: Reference to third party Application Guides

This section contains reference to third party Application Guides for VPN product. The documents for Avaya Application Guides are available for download from the Avaya Customer Support website: http://www.avaya.com/support.

- SSL VPN - Authentication using Steel Belted RADIUS server
- SSL VPN - NTLM Authentication
- SSL VPN - CRL retrieval
- SSL VPN - Configuring NetDirect
- SSL VPN - Authentication using certificates
- SSL VPN – Authentication using Netegrity SiteMinder
- SSL VPN - Syslog and Traffic log
- SSL VPN - External Authentication using Remote Authentication Dial-In User Service (RADIUS)
- SSL VPN - External LDAP Authentication using Active Directory
- SSL VPN - Configuring access rules
- SSL VPN - Adding links to a portal page
- SSL VPN - Configuring User Types SSL VPN - Configuring User Types
- Adding a Server Certificate and/or Private Key
- HTTP to HTTPS Redirect Service
- Using Netegrity SiteMinder with Avaya SSL VPN
- Technical Configuration Guide Using Citrix with the Alteon SSL VPN
- SSL VPN and SafeWord for Avaya Technical Config Guide

Chapter 9: Customer service

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

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to http://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 http://www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

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

Chapter 10: Syslog Messages

This appendix contains a list of the syslog messages that are sent from the Avaya VPN Gateway (AVG) to a Syslog server (when added to the system configuration). All the syslog messages follow common specifications. These messages are compliant with the SYSLOG SRD specifications. They can be stored locally on the hard disk or in a memory buffer. Syslog servers are added to the system configuration by using the menu options in the Syslog Servers menu. To view the menu options, see the *"Syslog Servers Configuration"* section under *Configuration Menu>System Configuration* in the *Avaya Command Reference*.

List of Syslog Messages

This section lists the Syslog messages that can be sent from a VPN Gateway to a configured Syslog server. The messages are divided into the following message types:

- Operating system (OS)
- System control
- Traffic processing
- Startup
- Configuration reload
- AAA
- IPsec

To view a list of syslog messages in alphabetical order, see the section Syslog Messages in Alphabetical Order on page 101.

Operating System (OS) Messages

The OS system messages are divided into three categories:

- EMERG
- CRITICAL
- ERROR

EMERG

- Root filesystem corrupt

  The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall to recover.

- Config filesystem corrupt beyond repair

  The system cannot boot, but stops with a single-user prompt. Reinstall to recover.

- Failed to write to config filesystem

  Probable hardware error. Reinstall.

CRITICAL

- Config filesystem re-initialized - reinstall required

  Reinstall.

- Application filesystem corrupt - reinstall required

  Reinstall.

ERROR

- **Config filesystem corrupt**

  Possible loss of configuration. Followed by the message **Config filesystem re-initialized - reinstall required** or **Config filesystem restored from backup**.

- **Missing files in config filesystem**

  Possible loss of configuration. Followed by the message **Config filesystem re-initialized - reinstall required** or **Config filesystem restored from backup**.

- **Logs filesystem re-initialized**

  Loss of logs.

- **Root filesystem repaired - rebooting**

  fsck found and fixed errors. Probably OK.

- **Config filesystem restored from backup**

  Loss of recent configuration changes.

- **Rebooting to revert to permanent OS version**

Happens after **Config filesystem re-initialized - reinstall required** or **Config filesystem restored from backup** if software upgrade is in progress (that is, if failure at first boot on new OS version).

System Control Process Messages

The System Control Process messages are divided into three categories:

- INFO
- ALARM
- EVENT

Both events and alarms are stored in the event log file, which can be accessed by typing the

```
/info/events/download
```

command. Active alarms can be viewed by typing the

```
/info/events/alarms
```

command.

INFO

System started [isdssl-<version>]

Sent whenever the system control process has been (re)started.

ALARM

Alarms are sent at a syslog level corresponding to the alarm severity as shown in the following table:

Alarm Severity	Syslog Level
CRITICAL	ALERT
MAJOR	CRITICAL
MINOR	ERROR
WARNING	WARNING
*	ERROR

Alarms are formatted according to the following pattern:

Id: <alarm sequence number> Severity: <severity> Name: <name of alarm> Time. <date and time of the alarm> Sender: <sender, e.g. system or the VPN Gateway IP address> Cause: <cause of the alarm> Extra: <additional information about the alarm>

To simplify finding the desired alarm messages, this section lists alarms with the **name** parameter on top.

- Name: **isd_down** Sender: <IP> Cause: down Extra: Severity: critical

  A member of the AVG cluster is down. This alarm is only sent if the cluster contains more than one VPN Gateway.

- Name: **single_master** Sender: system Cause: down Extra: Severity: warning

  Only one master VPN Gateway in the cluster is up and running.

- Name: **log_open_failed** Sender: <IP>, event Cause and Extra are explanations of the fault. Severity: major

  The event log (where all events and alarms are stored) could not be opened.

- Name: **make_software_release_permanent_failed** Sender: <IP> Cause: file_error | not_installed Extra: "Detailed info" Severity: critical

  Failed to make a new software release permanent after being activated. The system will automatically revert to the previous version.

- Name: **copy_software_release_failed** Sender: <IP> Cause: copy_failed | bad_release_package | no_release_package | unpack_failed Extra: "Detailed info" Severity: critical

  A VPN Gateway failed to install a software release while trying to install the same version as all other VPN Gateways in the cluster. The failing VPN Gateway tries to catch up with the other cluster members as it was not up and running when the new software version was installed.

- Name: **license** Sender: license_server Cause: license_not_loaded Extra: "All iSDs do not have the same license loaded " Severity: warning

  All VPN Gateways in the cluster do not have a license containing the same set of licensed features. Check loaded licenses using the

  ```
  /cfg/sys/cur
  ```

  command.

- Name: **license** Sender: <IP> Cause: license_expire_soon Extra: "Expires: <TIME> " Severity: warning

  The (demo) license loaded to the local VPN Gateway expires within 7 days. Check loaded licenses using the

  ```
  /cfg/sys/cur
  ```

  command.

- Name: **ssl_hw_fail** Sender: <IP> Cause: find_error |init_error Extra: Severity: major

  The SSL hardware acceleration card could not be found or initiated. This will cause the VPN Gateway to run with degraded performance.

- Name: **hsm_not_logged_in** Sender: <IP>, <Token> Cause: reboot Extra: "Card<Token> " Severity: critical

  After a reboot, login to the HSM card is required.

- Name: **hsm_tampered_with** Sender: <IP>, <Token> Cause: hsm_detected Extra: "Card<Token> " Severity: critical

- Name: **slave_not_starting** Sender: <IP>, <SlaveNo> Cause: start_error | connect_timeout | fdsend | nothidden | name_resolv | nodename_occupied Extra:" Severity: warning

  The portal handling subsystem cannot be started.

When an alarm is cleared, one of the following messages are sent:

Alarm Cleared Name="<Name>" Id="<ID>" Sender="<Sender>" Alarm Cleared Id="<ID>"

EVENT

Events are sent at the NOTICE syslog level. They are formatted according to the following pattern:

Name: <Name> Sender: <Sender> Extra: <Extra>

- Name: **partitioned_network** Sender and Extra is lower level information.

  Sent to indicate that a VPN Gateway is recovering from a partitioned network situation.

- Name: **ssi_mipishere** Sender: ssi Extra: <IP>

  Tells that the MIP (management IP address) is now located at the VPN Gateway with the <IP> host IP address.

- Name: **license_expire_soon** Sender: <IP>

  Indicates that the loaded (demo) license at the <IP> VPN Gateway expires within 7 days.

- Name: **aaa_license_exhausted** Sender: <IP>:<VPNIndex> Extra: ssl | IPsec

  This event is sent when the VPN has run out of SSL or IPsec user licenses. A hysteris mechanism is used so that no more than one event per hour is sent for one VPN.

  If <VPNIndex> is 0, the globally shared license was exhausted.

- Name: **software_configuration_changed** Sender: system Extra: software release version <VSN> <Status> Indicates that release <VSN> (version) has been <Status> (unpacked/installed/permanent).

- Name: **software_release_copying**Sender: <IP> Extra: copy software release <VSN> from other cluster member

  Indicates that <IP> is copying the release <VSN> from another cluster member.

- Name: **software_release_rebooting** Sender: <IP> Extra: reboot with release version <VSN>

  Indicates that a VPN Gateway (<IP>) is rebooting on a new release (that is, a VPN Gateway that was not up and running during the normal installation is now catching up).

- Name: **license_expired** Sender = <IP>

  Indicates that the demo license loaded at host <IP> has expired. Check the loaded licenses with

  ```
  /cfg/sys/cur
  ```

  .

- Name: **audit** Sender: CLI Extra: Start <session> <details> Update <session> <details> Stop <session> <details>

  Sent when a CLI system administrator enters, exits or updates the CLI if audit logging is enabled using the

  ```
  /cfg/sys/adm/audit/ena
  ```

  command.

Traffic Processing Messages

The Traffic Processing Subsystem messages are divided into these categories:

- CRITICAL
- ERROR
- WARNING
- INFO

CRITICAL

DNS alarm: all dns servers are DOWN

All DNS servers are down. The VPN Gateway cannot perform any DNS lookups.

ERROR

- **internal error: <no>**

  An internal error occurred. Contact support with as much information as possible to reproduce this message.

- **javascript error: <reason> for: <host><path>**

  JavaScript parsing error encountered when parsing content from <host><path>. This could be a problem in the AVG JavaScript parser, but most likely a syntactical error in the JavaScript on that page.

- **vbscript error: <reason> for: <host><path>**

  VBScript parsing error encountered when parsing content from <host><path>. This could be a problem in the AVG VBScript parser, but most likely a syntactical error in the VBScript on that page.

- **jscript.encode error: <reason>**

  Problem encountered when parsing an encoded JavaScript. It may be a problem with the JavaScript parser in the AVG or it could be a problem on the processed page.

- **css error: <reason>**

  Problem encountered when parsing an style sheet. It may be a problem with the css parser in the AVG or it could be a problem on the processed page.

- **Failed to syslog traffic :<reason> -- disabling traf log**

  Problem occurred when the AVG tried to send traffic logging syslog messages. Traffic syslogging was disabled as a result.

- **www_authenticate: bad credentials**

  The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.

- **http error: <reason>, Request="<method> <host><path>"**

  A problem was encountered when parsing the HTTP traffic. This is either an indication of a non-standard client/server or an indication that the AVG's HTTP parser has gotten out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.

- **http header warning cli: <reason> (<header>)**

  The client sent a bad HTTP header.

- **http header warning srv: <reason> (<header>)**

  The server sent a bad HTTP header.

- **unknown WWW-Authenticate method, closing**

  Backend server sent unknown HTTP authentication method.

- **failed to parse Set-Cookie <header>**

  The AVG got a malformed Set-Cookie header from the backend Web server.

- **failed to locate corresponding portal for portal authenticated http server**

  Portal authentication has been configured for an http server, but no portal using the same VPN can be found. Make sure that there is a portal running using the same VPN id.

- **Bad IP:PORT data <line> in hc script**

  Bad ip:port found in health check script. Reconfigure the health script. This should normally be captured earlier by the CLI.

- **Bad regexp (<expr>) in health check**

  Bad regular expression found in health check script. Reconfigure. This should normally be captured earlier by the CLI.

- **Bad script op found <script op>**

  Bad script operation found in health check script. Reconfigure. This should normally be captured earlier by the CLI.

- **Bad string found <string>**

  Bad load balancing string encountered. This is normally verified by the CLI.

- **Unable to use the certificate for <server nr>**

  Unsuitable certificate configured for server #.

- **The private key and certificate don't match for <server nr>**

  Key and certificate does not match for server #. The certificate has to be changed.

- **Unable to use client private key for <server #>**

  Key for doing sslconnect is not valid. Reconfigure.

- **Unable to find client private key for <server #>**

  Key for doing sslconnect is not valid. Reconfigure.

- **Unable to use client certificate for <server #>**

  Certificate for doing sslconnect is not valid. Reconfigure.

- **Failed to initialize SSL hardware**

  Problem initializing SSL acceleration hardware. This will cause the VPN Gateway to run with degraded performance.

- **Could not find SSL hardware.**

Failed to detect SSL acceleration hardware.

- **Connect failed: <reason>**

  Connect to backend server failed with <reason>

- **SSL connect failed: <reason>**

  SSL connect to backend server failed with <reason>

- **html error: <reason>**

  Error encountered when parsing HTML. Probably non-standard HTML.

- **socks error: <reason>**

  Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.

- **socks request: socks version <version> rejected**

  Socks request of version <version> received and rejected. Most likely a non-standard socks client.

- **Failed to log to CLI:<reason> -- disabling CLI log**

  Failed to send troubleshooting log to CLI. Disabling CLI troubleshooting log.

- **Can't bind to local address: <ip>:<port>: <reason>**

  Problem encountered when trying to set up virtual server on <ip>:<port>.

- **Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>**

  AVG received reply for non-configured DNS server.

- **Proxy connect host name too long: <host>**

  The host name is too long to perform proxy connect. Make the host name shorter or remove the domain from the proxy connect mapping.

- **Certificate CRL handling errors:**

  - failed to start auto-crl handling
  - <Cert#>: syntax error when parsing the CRL-URL
  - <Cert#>: automatic retrieval of HTTP-CRL failed - lookup failure <Host>
  - <Cert#>: automatic retrieval of HTTP-CRL failed - parse error
  - <Cert#>: auto-crl over HTTP failed, reason: <Reason>
  - <Cert#>: automatic retrieval of HTTP-CRL failed
  - <Cert#>: failed to create TFTP-CRL temp file
  - <Cert#>: parsing of TPFP-CRL URL failed
  - <Cert#>: automatic retrieval of TFTP-CRL failed - lookup failure <Host>

- <Cert#>: failed to read TFTP-CRL temp file
- <Cert#>: automatic retrieval of TFTP-CRL failed
- <Cert#>: automatic retrieval of LDAP-CRL failed - lookup failure <Host>
- <Cert#>: failed to contact LDAP server at <Host>
- <Cert#>: no CRL (1) found at LDAP server
- <Cert#>: CRL authentication failed
- <Cert#>: no CRL (2) found at LDAP server
- <Cert#>: no CRL (3) found at LDAP server
- <Cert#>: no CRL passwd found
- <Cert#>: no CRL filter was found
- <Cert#>: no CRL interval found for cert
- <Cert#>: CRL revocation failed - <Reason>

WARNING

- TPS license limit (<limit>) exceeded

  The transactions per second (TPS) limit has been exceeded.
- No PortalGuard license loaded: VPN <id> *will* use portal authentication

  The PortalGuard license has not been loaded on the VPN Gateway but

  ```
  /cfg/vpn # /server/portal/authenticate
  ```

  is set to

  ```
  off
  ```

  .
- No Secure Service Partitioning loaded: server <id> *will not* use interface <n>

  The Secure Service Partitioning license has not been loaded on the VPN Gateway but the server is configured to use a specific interface.
- License expired

  The loaded (demo) license on the VPN Gateway has expired. The VPN Gateway now uses the default license.
- Server <id> uses default interface (interface <n> not configured)

  A specific interface is configured to be used by the server but this interface is not configured on the VPN Gateway.
- IPSEC server <id> uses default interface (interface <n> not configured)

A specific interface is configured to be used by the IPsec server but this interface is not configured on the VPN Gateway.

- Certificate CRL handling warnings:
  - <Cert#>: no CRL-URL specified
  - invalid escape sequence in DN, ignoring...
  - <Cert#>: Ambiguous CRL configuration, all usage of certificate <Cert> does not bind to the same interface and/or DNS environment - using gateway <Gateway> settings

INFO

- gzip error: <reason>

  Problem encountered when processing compressed content.

- gzip warning: <reason>

  Problem encountered when processing compressed content.

- accept() turned off (<nr>) too many fds

  The VPN Gateway has temporarily stopped accepting new connections. This will happen when the VPN Gateway is overloaded. It will start accepting connections once it has finished processing its current sessions.

- No cert supplied by backend server

  No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.

- No CN supplied in server cert <subject>

  No CN found in the subject of the certificate supplied by the backend server.

- Bad CN supplied in server cert <subject>

  Malformed CN found in subject of the certificate supplied by the backend server.

- Shutting sslproxy down.

  Traffic subsystem has been stopped.

- Restarting proxy due to <reason>

  Traffic subsystem restarted due to <reason>

- DNS alarm: dns server(s) are UP

  At least one DNS server is now up.

- HC: backend <ip>:<port> is down

Backend health check detected backend <ip>:<port> to be down.

- HC: backend <ip>:<port> is up again

  Backend health check detected backend <ip>:<port> to be up.

Startup Messages

The Traffic Processing Subsystem Startup messages only include the INFO category.

INFO

- HSM mode: <mode>

  Hardware Security Mode <mode>.

- Disabling transparent proxy, non-compatible with pooling

  Transparent proxy mode is disabled due to pooling being enabled (startup message).

- Set CSWIFT as default

  Using CSWIFT SSL hardware acceleration. (startup message).

- Using <hwtype> hardware

  Using <hwtype> hardware for SSL acceleration. (startup message)

- Loaded <ip>:<port>

  Initializing virtual server <ip>:<port>.

- Because we use clicerts, force adjust totalcache size to: <size> per server that use clicerts

  Generated if the size of the SSL session cache has been modified.

- No more than <nr> backend supported

  Generated when more than the maximum allowed backend servers have been configured.

- TPS license limit: <limit>

  TPS limit set to <limit>

- No TPS license limit

  Unlimited TPS license used.

- Started ssl-proxy

  Traffic subsystem started.

- Found <size> meg of phys mem

Amount of physical memory found on system.

Configuration Reload Messages

The Traffic Subsystem Configuration Reload messages only include the INFO category.

INFO

- reload cert config start

  Starting reloading of certificates.
- reload cert config done

  Certificate reloading done.
- reload configuration start

  Virtual server configuration reloading start.
- reload configuration network down

  Accepting new sessions are temporarily put on hold.
- reload configuration network up

  Resuming accepting new sessions after loading new configuration.
- reload configuration done

  Virtual server configuration reloading done.

AAA Subsystem Messages

The AAA (Authentication, Authorization and Accounting) subsystem messages are divided into these categories:

- ERROR
- WARNING
- INFO

ERROR

LDAP backend(s) unreachable Vpn=\"<id>\" AuthId=\"<authid>\"

In case LDAP server(s) cannot be reached when a user tries to login to the Portal.

WARNING

Host <host ip> has been down too long: is no longer accounted for in the license pool.

The host has been down too long (more than 30 days) and is no longer accounted for in the license pool.

INFO

Host <host ip> is up: accounted for in the license pool.

A host that has been down too long is up again and is now sharing its licenses in the license pool.

Log functionality

Messages listed are generated if the CLI command

```
/cfg/vpn #/adv/log
```

is enabled.

If the log value contains

```
login
```

, the following messages can be displayed:

- VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>"
- VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>" TunIP="<inner tunnel ip>"
- VPN AddressAssigned Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" TunIP="<inner tunnel ip>"
- VPN LoginFailed Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" [User="<user>"] Error=<error>
- VPN Logout Vpn="<id>" SrcIp="<ip>" User="<user>"

If the log value contains

```
portal
```

, the following messages can be displayed:

PORTAL Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"

If the log value contains

```
http
```

, the following messages can be displayed:

- HTTP Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"
- HTTP NotLoggedIn Vpn="<id>" Host="<host>" SrcIP="<ip>" Request="<method> <host> <path>"

If the log value contains

```
socks
```

, the following messages can be displayed:

SOCKS Vpn="<id>" User="<user>" SrcIP="<ip>" Request="<request>"

This message refers to the features on the Portal's Advanced tab.

If the log value contains

```
reject
```

, the following messages can be displayed:

- HTTP Rejected Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"
- PORTAL Rejected Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"
- SOCKS Rejected Vpn="<id>" User="<user>" SrcIP="<ip>" Request="<request>"

IPsec Subsystem Messages

The IPsec subsystem messages are divided into these categories:

- ERROR
- WARNING
- NOTICE
- INFO

ERROR

There are several ERROR messages that may get sent from the IPsec subsystem. They all indicate internal errors and thus provide no meaningful information for troubleshooting.

WARNING

- CreateSession Failed with sessionId 0

  AAA returned failure for creating session.
- Can't find new IKE Profile %s received in Auth Reply

  AAA provided new IKE profile as received from RADIUS, but IKE does not have it.
- Log off notif for non-existing session id %u

  AAA notified about log-off for a non-existing session.
- Quick mode initiation to %s failed, error - %s

  Quickmode initiation failed.
- All credits are exhausted for Isakmp SA

  Maximum number of outstanding ISAKMP SA create requests have exceeded the limit.
- All credits are exhausted for IPSec SA

  Maximum number of outstanding IPsec SA create requests have exceeded the limit.
- Ignoring unauthenticated informational message from %s

  Dropping message without the authentication hash.
- Dropping unprotected notify message %s from %s

  Dropping the clear-text notify message.
- IPsec Mobility is disabled. Roaming request denied.

  Dropping the roaming request. Mobility is disabled in the configuration.
- Malformed ADDRESS_CHANGE notify message received from %s

  Dropping invalid ADDRESS_CHANGE (Mobility) request.
- Message from %s dropped because SPI is not found

  Dropping message because SPI is not found.
- Ignoring request to roam from %s to %s due to invalid source. Expecting %s

  Dropping roam request message because mismatch in source in payload and header.
- Ignoring request to roam from %s to %s

  Dropping roam request because old and new source IP are same.
- Error in Diffie-Hellman Setup, group=%u

  Error in DH Setup.

- No IPsec encryption type selected for %s - terminating connection attempt

  IPsec encryption does not match with the configured value.

- Diffie-Hellman group mismatch for %s - terminating connection attempt

  Configured Diffie-Hellman Group does not match with the one that the peer requested.

- PFS is required but not provided by %s

  PFS (Perfect Forward Secrecy) is configured locally, but the peer does not provide it.

- No Secure Service Partitioning license loaded IPSEC server ~s *will not* use interface ~p

  Secure Service Partitioning license not loaded.

- IPsec server ~s uses default interface (interface ~p not configured)

  This indicates possible badly configured default gateways on some Secure Service Partitioning interface.

- Failed to allocate IP addr from empty pool

  The IP address pool is empty and a login attempt was rejected due to not being able to allocate an IP address from the pool. Note that Net Direct clients also use IPs from the IP pool.

NOTICE

- Failed to decode client cert

  A client sent a bad client certificate which could not decoded/parsed.

- Bad clicert, Can't find issuer in clicert

  A client sent a bad client certificate which did not contain an issuer.

- Error while decoding certificate DER Id

  A client sent a certificate where the X509 Name portion could not be extracted from the certificate.

- Client cert %d revoked

  The client certificate with serial number %d was revoked and thus login failed.

- Ike not started due: No license

  If no licence can be found (such as on old ASA 310), IKE is not started.

INFO

- Using new IKE. IKE Profile %s received in Auth Reply.

Received new IKE profile from AAA (received from RADIUS).

- ISAKMP SA Established with %s

  ISAKMP SA Established.

- IPSec SA Established with %s, IPComp %s, inbound CPI 0x%x

  IPsec SA Established.

- Closing earlier opened UDP Encap Socket for port : %d

  UDP Encap port number changed.

- Creating UDP Encap Socket for %d.%d.%d.%d/%d

  UDP Encap port number changed.

- Received Delete ISAKMP SA message from %s

  Received Delete ISAKMP SA message.

- Received Delete IPSEC SA message from %s

  Received Delete IPsec SA message.

- Client %s rejected IPSec SA Proposal, so deleting ISAKMP SA

  Client rejected the IPSec SA proposal.

- Deleting the QM replaced by new rekeyed QM

  Deleting the old IPsec SA which has been replaced with the new rekeyed one.

- No response from %s for maximum retransmission attempts %d

  Maximum number of retransmission attempts reached.

- ike Connected successfully to erlang

  IKE daemon has started and connected to the registry database.

- revocation byte length: %d

  Loading certificate revocation list of length %d.

- Loaded ca certificate %s

  Loaded CA certificate with name %s. This certificate is used to verify client certificates.

- Loaded server cert %s

  Loaded server certificate with name %s. This certificate must be signed by a trusted CA in the client.

- Creating Ike Profile %s

  Creating/Loading a new IKE profile called %s.

- Updating Ike profile %s

A CLI/BBI change in IKE profile %s forces an update of the profile.

- Deleting ike profile %s

  IKE profile %s has been deleted in the CLI or BBI.

- Creating tunnel profile %s

  Updating tunnel profile %s.

- Deleting tunnel profile %s

  Deleting tunnel profile %s.

- Bad clientcert, no matching ca cert found

  A client tried to login with a client certificate when the corresponding CA certificate was not loaded in IKE.

- failed rsa private encrypt

  Failure to encrypt data while signing with the CA certificate.

- Failed to certificate der encode

  Failed to der encode the CA certificate.

- Allocated IP .....

  An IP address was allocated from the IP pool.

- Returned IP .....

  An IP address was returned to the IP address pool.

SPO Client

This section shows the various syslog messages for the SPO client.

```
[30 Jan 2008 20:49:15] ************************************
[30 Jan 2008 20:49:15] Starting SPO Client Version 7.1.0.20 [30 Jan 2008
20:49:15] ************************************
/*File Locations For SPOCLient*/
[30 Jan 2008 20:49:15] Info : LogLocation : E:\projectusb\SRC\USBClient
\release\SPOClient.log
[30 Jan 2008 20:49:15] Info : ConfigFileLocation : E:\projectusb\SRC
\USBClient\release\Config\config.ini
[30 Jan 2008 20:49:15] Info : LangFileLocation : E:\projectusb\SRC
\USBClient\release\Lang\
[30 Jan 2008 20:49:15] Info : SkinFileLocation : E:\projectusb\SRC
\USBClient\release\skin\
[30 Jan 2008 20:49:15] Info : AppsDirectoryLocation : E:\projectusb\SRC
\USBClient\release\Apps\
[30 Jan 2008 20:49:15] Info : g_csAppLocation : E:\projectusb\SRC
\USBClient\release\
[30 Jan 2008 20:49:15] Info : g_csUsbTempPath :E:\projectusb\SRC\USBClient
```

```
\release\Temp\
/*File Locations For SPOCLient*/
[30 Jan 2008 20:49:15] Info : SetProfileStatusText
/*Making HTTPS Request to get Auth XML*/
[30 Jan 2008 20:49:17] Info : Sending Https Request
[30 Jan 2008 20:49:29] Info : Reading Response from server
[30 Jan 2008 20:49:29] Info : Reading Response from server
[30 Jan 2008 20:49:29] Info : SendHttpsRequest Successes
/*Making HTTPS Request to get Auth XML*/
/*Loading and Parsing the Auth XML*/
[30 Jan 2008 20:49:29] Info : Loading AuthType XML File
[30 Jan 2008 20:49:29] Info : Loading AuthType XML File 1
[30 Jan 2008 20:49:29] Info : Loading AuthType XML File 2
[30 Jan 2008 20:49:29] Info : Loading AuthType XML File 3
[30 Jan 2008 20:49:29] Info : Loading AuthType XML File 4
[30 Jan 2008 20:49:29] Info : Loading AuthType XML File 5
/*Loading and Parsing the Auth XML*/
/*Downloading Logo And SysIcon Files*/
[30 Jan 2008 20:49:29] Info : Sending Https Request
[30 Jan 2008 20:49:29] Info : Reading Response from server
[30 Jan 2008 20:49:29] Info : Reading Response from server
[30 Jan 2008 20:49:29] Info : Reading Response from server
[30 Jan 2008 20:49:29] Info : SendHttpsRequest Successes
[30 Jan 2008 20:49:29] Info : Sending Https Request
[30 Jan 2008 20:49:29] Info : Reading Response from server
[30 Jan 2008 20:49:29] Info : Reading Response from server
[30 Jan 2008 20:49:29] Info : SendHttpsRequest Successes
/*Downloading Logo And SysIcon Files*/
[30 Jan 2008 20:49:29] Info : Loading AuthList
/*Authentication Through Socks*/
[30 Jan 2008 20:49:33] Info : Server Response: 2 Bytes.5 d2
[30 Jan 2008 20:49:34] Info : Sending Auth Request
[30 Jan 2008 20:49:34] Info : Server Response: 68 Bytes.1 4 0 1 0 80 22
61 64 36 31 32 38 38 36 37 35 35 34 31 33 2e 32 33 30 34 38 38 38 33 37
39 32 36 39 36 31 35 38 37 33 88 16 33 63 34 62 34 33 38 30 35 35 39 31
31 32 31 37 33 31 35 38 34 31 8a 1 0
[30 Jan 2008 20:49:34] Info : Reading Cookie from the server
[30 Jan 2008 20:49:34] Info : Reading secret from the server
/*Authentication Through Socks*/
[30 Jan 2008 20:49:34] Info : Intializing TG Dialog
[30 Jan 2008 20:49:34] Info : Retrunging TG Dialog
[30 Jan 2008 20:49:34] Info : Waitfor single object executed
/*Https Request to home.yaws*/
[30 Jan 2008 20:49:34] Info : Sending Https Request
[30 Jan 2008 20:49:34] Info : Reading Response from server
[30 Jan 2008 20:49:34] Info : Reading Response from server
[30 Jan 2008 20:49:34] Info : Reading Response from server
[30 Jan 2008 20:49:34] Info : SendHttpsRequest Successes
/*Https Request to home.yaws*/
/*Parsing Linkset XML*/
[30 Jan 2008 20:49:34] Info : Loading Link XML File
[30 Jan 2008 20:49:34] Info : Linkset retrieved from XML
[30 Jan 2008 20:49:34] Info : Linkset retrieved from XML /*Parsing Linkset
XML*/ [30 Jan 2008 20:49:35] Info : Starting DashBoard
[30 Jan 2008 20:49:35] Info : Starting Traydailog
[30 Jan 2008 20:49:36] Info : Refreshing User Links
/*User Links that were not added as a result of bad path*/
[30 Jan 2008 20:49:36] Warning : User Link ert Not Added.Please Verify Path
[30 Jan 2008 20:49:37] Warning : User Link dfgd Not Added.Please Verify
Path  [30 Jan 2008 20:49:37] Warning : User Link dsfds Not Added.Please
Verify Path  [30 Jan 2008 20:49:37] Warning : User Link sdf Not
Added.Please Verify Path
[30 Jan 2008 20:49:37] Warning : User Link dfg Not Added.Please Verify Path
```

```
[30 Jan 2008 20:49:37] Warning : User Link sdfds Not Added.Please Verify
Path  [30 Jan 2008 20:49:37] Warning : User Link dsfg Not Added.Please
Verify Path
[30 Jan 2008 20:49:37] Warning : User Link fgfd Not Added.Please Verify
Path
[30 Jan 2008 20:49:37] Warning : User Link sdf Not Added.Please Verify Path
[30 Jan 2008 20:49:37] Warning : User Link dfg Not Added.Please Verify Path
[30 Jan 2008 20:49:37] Warning : User Link sdfd Not Added.Please Verify
Path  [30 Jan 2008 20:49:37] Warning : User Link fdg Not Added.Please
Verify Path
[30 Jan 2008 20:49:37] Warning : User Link dfg Not Added.Please Verify Path
[30 Jan 2008 20:49:37] Warning : User Link sdfsd Not Added.Please Verify
Path  [30 Jan 2008 20:49:37] Warning : User Link fgh Not Added.Please
Verify Path
[30 Jan 2008 20:49:37] Warning : User Link dsf Not Added.Please Verify Path
[30 Jan 2008 20:49:37] Warning : User Link fdg Not Added.Please Verify Path
[30 Jan 2008 20:49:37] Warning : User Link eew Not Added.Please Verify
Path /*User Links that were not added as a result of bad path*/
/*User Links that were added*/
[30 Jan 2008 20:49:37] Info : UserLink ID  0
[30 Jan 2008 20:49:37] Info : UserLink Link Name  telnet
[30 Jan 2008 20:49:37] Info : UserLink Link Name  C:\WINNT\system32\CMD.EXE
[30 Jan 2008 20:49:37] Info : UserLink ID  1
[30 Jan 2008 20:49:37] Info : UserLink Link Name  test12
[30 Jan 2008 20:49:37] Info : UserLink Link Name  C:\WINNT
\system32\telnet.exe [30 Jan 2008 20:49:37] Info : UserLink ID  2
[30 Jan 2008 20:49:37] Info : UserLink Link Name  cmd
[30 Jan 2008 20:49:37] Info : UserLink Link Name  C:\WINNT
\system32\CMD.EXE /*User Links that were added*/
[30 Jan 2008 20:49:37] Info : Setting UserLink Html
[30 Jan 2008 20:49:37] Info : Setting  TRAY UserLink Html
[30 Jan 2008 20:49:37] Info : Setting  TRAY UserLink Html 1
[30 Jan 2008 20:49:37] Info : Updating Tool Tip Status
[30 Jan 2008 20:49:37] Info : Refreshing SSL Session
[30 Jan 2008 20:49:37] Info : Sending Https Request
[30 Jan 2008 20:49:37] Info : Reading Response from server
[30 Jan 2008 20:49:37] Info : Reading Response from server
[30 Jan 2008 20:49:37] Info : SendHttpsRequest Successes
[30 Jan 2008 20:49:37] Info : Updating Status Tab
[30 Jan 2008 20:49:37] Info : Refreshing SSL Session
[30 Jan 2008 20:49:37] Info : Sending Https Request
[30 Jan 2008 20:49:37] Info : Reading Response from server
[30 Jan 2008 20:49:37] Info : Reading Response from server
[30 Jan 2008 20:49:37] Info : SendHttpsRequest Successes
/*Server Links that were retrieved from the server*/
[30 Jan 2008 20:49:37] Info : Refreshing Linksets
[30 Jan 2008 20:49:37] Info : Displaying Links
[30 Jan 2008 20:49:37] Info : test
[30 Jan 2008 20:49:37] Info : vdesktop_test
[30 Jan 2008 20:49:37] Info : wts
[30 Jan 2008 20:49:37] Info : netdirect
[30 Jan 2008 20:49:37] Info : customPf
[30 Jan 2008 20:49:37] Info : customnd
[30 Jan 2008 20:49:37] Info : customPftest
[30 Jan 2008 20:49:37] Info : test1
[30 Jan 2008 20:49:37] Info : ftp /*Server Links that were retrieved from
the server*/
[30 Jan 2008 20:49:39] Info : Refreshing SSL Session
[30 Jan 2008 20:49:39] Info : Sending Https Request
[30 Jan 2008 20:49:39] Info : Reading Response from server
[30 Jan 2008 20:49:39] Info : Reading Response from server
[30 Jan 2008 20:49:39] Info : SendHttpsRequest Successes
[30 Jan 2008 20:49:39] Info : Starting Link
```

```
[30 Jan 2008 20:49:39] Info : 1 [30 Jan 2008 20:49:39] Info : test
[30 Jan 2008 20:49:39] Info : /xnet/ftp/172.16.3.16
[30 Jan 2008 20:50:37] Info : Refreshing SSL Session [30 Jan 2008
20:50:37] Info : Refreshing SSL Session
[30 Jan 2008 20:50:37] Info : Sending Https Request
[30 Jan 2008 20:50:37] Info : Reading Response from server
[30 Jan 2008 20:50:37] Info : Reading Response from server
[30 Jan 2008 20:50:37] Info : SendHttpsRequest Successes
[30 Jan 2008 20:50:37] Info : Refreshing SSL Session
[30 Jan 2008 20:50:37] Info : Sending Https Request
[30 Jan 2008 20:50:37] Info : Reading Response from server
[30 Jan 2008 20:50:37] Info : Reading Response from server
[30 Jan 2008 20:50:37] Info : SendHttpsRequest Successes
[30 Jan 2008 20:50:37] Info : Refreshing SSL Session
[30 Jan 2008 20:50:37] Info : Sending Https Request
[30 Jan 2008 20:50:37] Info : Reading Response from server
[30 Jan 2008 20:50:37] Info : Reading Response from server
[30 Jan 2008 20:50:37] Info : SendHttpsRequest Successes
/*Closing SPOClient*/
[30 Jan 2008 20:50:44] Info : Calling Java Script to Close Windows
[30 Jan 2008 20:50:44] Info : Logging out
[30 Jan 2008 20:50:44] Info : Sending Https Request
[30 Jan 2008 20:50:44] Info : Reading Response from server
[30 Jan 2008 20:50:44] Info : Reading Response from server
[30 Jan 2008 20:50:44] Info : SendHttpsRequest Successes
/*Closing SPOClient*/
```

Error Messages

Message	Error Code	Problem Cause	Resolution
In Windows VISTA environment if you get a message inside virtual desktop for example "You must be an administrator to open Internet Explorer on this desktop." To open Internet Explorer, right-click the Internet Explorer icon, and then click 'Run as administrator'.	-	This problem occurs because some security enhancements in Windows Vista prevent the user from starting Internet Explorer on a desktop (virtual desktop) that is not the default desktop.	Install the microsoft patch http://support.microsoft.com/kb/935855/ and add the SPO server site into vista IE trusted site.

Syslog Messages in Alphabetical Order

This section lists the syslog messages in alphabetical order.

Table 7: Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
aaa_license_exhausted	EVENT	System Control	This event is sent when the VPN has run out of SSL or IPsec user licenses. A hysteris mechanism is used so that no more than one event per hour is sent for one VPN. If <VPNIndex> is 0, the globally shared license was exhausted.
accept() turned off (<nr>) too many fds	INFO	Traffic Processing	The VPN Gateway has temporarily stopped accepting new connections. This will happen when the VPN Gateway is overloaded. It will start accepting connections once it has finished processing its current sessions.
All credits are exhausted for IPSec SA	WARNING	IPsec	Maximum number of outstanding IPsec SA create requests have exceeded the limit.
All credits are exhausted for Isakmp SA	WARNING	IPsec	Maximum number of outstanding ISAKMP SA create requests have exceeded the limit.

Message	Severity	Type	Explanation
Allocated IP	INFO	IPsec	An IP address was allocated from the IP pool.
Application filesystem corrupt - reinstall required	CRITICAL	OS	Reinstall.
audit	EVENT	System Control	Sent when a CLI system administrator enters, enters, exits or updates the CLI if audit logging is enabled using the **/cfg/sys/adm/audit /ena** command.
Bad clicert, Can't find issuer in clicert	NOTICE	IPsec	A client sent a bad client certificate which did not contain an issuer.
Bad clientcert, no matching ca cert found	INFO	IPsec	A client tried to login with a client certificate when the corresponding CA certificate was not loaded in IKE.
Bad CN supplied in server cert <subject>	INFO	Traffic Processing	Malformed CN found in subject of the certificate supplied by the backend server.
Bad IP:PORT data <line> in hc script	ERROR	Traffic Processing	Bad ip:port found in health check script. Reconfigure the health script. This should normally be captured earlier by the CLI.
Bad regexp (<expr>) in health check	ERROR	Traffic Processing	Bad regular expression found in health check script. Reconfigure. This should normally be captured earlier by the CLI.

Message	Severity	Type	Explanation
Bad script op found <script op>	ERROR	Traffic Processing	Bad script operation found in health check script. Reconfigure. This should normally be captured earlier by the CLI.
Bad string found <string>	ERROR	Traffic Processing	Bad load balancing string encountered. This is normally verified by the CLI.
Can't bind to local address: <ip>:<port>: <reason>	ERROR	Traffic Processing	Problem encountered when trying to set up virtual server on <ip>:<port>.
Can't find new IKE Profile %s received in Auth Reply	WARNING	IPsec	AAA provided new IKE profile as received from RADIUS, but IKE does not have it.
Client %s rejected IPSec SA Proposal, so deleting ISAKMP SA	INFO	IPsec	Client rejected the IPSec SA proposal.
Client cert %d revoked	NOTICE	IPsec	The client certificate with serial number %d was revoked and thus login failed.
Closing earlier opened UDP Encap Socket for port: %d	INFO	IPsec	UDP Encap port number changed.
Config filesystem corrupt	ERROR	OS	Possible loss of configuration. Followed by the message `Config filesystem re-initialized - reinstall required` or `Config filesystem restored from backup`.

Message	Severity	Type	Explanation
Config filesystem corrupt beyond repair	EMERG	OS	The system cannot boot, but stops with a single-user prompt. Reinstall to recover.
Config filesystem re-initialized - reinstall required	CRITICAL	OS	Reinstall.
Config filesystem restored from backup	ERROR	OS	Loss of recent configuration changes.
Connect failed: <reason>	ERROR	Traffic Processing	Connect to backend server failed with <reason>.
copy_software_release_failed	ALARM (CRITICAL)	System Control	A VPN Gateway failed to install a software release while trying to install the same version as all other VPN Gateway(s) in the cluster. The failing VPN Gateway tries to catch up with the other cluster members as it was not up and running when the new software version was installed.
Could not find SSL hardware.	ERROR	Traffic Processing	Failed to detect SSL acceleration hardware.
CreateSession Failed with sessionId 0	WARNING	IPsec	AAA returned failure for creating session.
Creating Ike Profile %s	INFO	IPsec	Creating/Loading a new IKE profile called %s.
Creating tunnel profile %s	INFO	IPsec	Updating tunnel profile %s.
Creating UDP Encap Socket for %d.%d. %d.%d/%d	INFO	IPsec	UDP Encap port number changed.

Message	Severity	Type	Explanation
css error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing an style sheet. It may be a problem with the css parser in the AVG or it could be a problem on the processed page.
Deleting ike profile %s	INFO	IPsec	IKE profile %s has been deleted in the CLI or BBI.
Deleting the QM replaced by new rekeyed QM	INFO	IPsec	Deleting the old IPsec SA which has been replaced with the new rekeyed one.
Deleting tunnel profile %s	INFO	IPsec	Deleting tunnel profile %s.
Diffie-Hellman group mismatch for %s - terminating connection attempt	WARNING	IPsec	Configured DH Group does not match with the one that the peer requested.
Disabling transparent proxy, non-compatible with pooling	INFO	Startup	Transparent proxy mode is disabled due to pooling being enabled.
DNS alarm: all dns servers are DOWN	CRITICAL	Traffic Processing	All DNS servers are down. The VPN Gateway cannot perform any DNS lookups.
DNS alarm: dns server(s) are UP	INFO	Traffic Processing	At least one DNS server is now up.
Dropping unprotected notify message %s from %s	WARNING	IPsec	Dropping the clear-text notify message.
Error in Diffie-Hellman Setup, group=%u	WARNING	IPsec	Error in DH Setup.
Error while decoding certificate DER Id	NOTICE	IPsec	A client sent a certificate where the

Message	Severity	Type	Explanation
			X509 Name portion could not be extracted from the certificate.
failed rsa private encrypt	INFO	IPsec	Failure to encrypt data while signing with the CA certificate.
Failed to allocate IP addr from empty pool	WARNING	IPsec	The IP address pool is empty and a login attempt was rejected due to not being able to allocate an IP address from the pool. Note that Net Direct clients also use IPs from the IP pool.
Failed to decode client cert	NOTICE	IPsec	A client sent a bad client certificate which could not decoded/parsed.
Failed to der encode certificate	INFO	IPsec	Failed to DER encode the CA certificate.
Failed to initialize SSL hardware	ERROR	Traffic Processing	Problem initializing SSL acceleration hardware. This will cause the VPN Gateway to run with degraded performance.
failed to locate corresponding portal for portal authenticated http server	ERROR	Traffic Processing	Portal authentication has been configured for an http server, but no portal using the same VPN id can be found. Make sure that there is a portal running using the same VPN id.
Failed to log to CLI:<reason> -- disabling CLI log	ERROR	Traffic Processing	Failed to send troubleshooting log to CLI. Disabling CLI troubleshooting log.

Message	Severity	Type	Explanation
failed to parse Set-Cookie <header>	ERROR	Traffic Processing	The AVG got a malformed Set-Cookie header from the backend web server.
Failed to syslog traffic:<reason> -- disabling traf log	ERROR	Traffic Processing	Problem occurred when the AVG tried to send traffic logging syslog messages. Traffic syslogging was disabled as a result.
Failed to write to config filesystem	EMERG	OS	Probable hardware error. Reinstall.
Found <size> meg of phys mem	INFO	Startup	Amount of physical memory found on system.
gzip error: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
gzip warning: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
HC: backend <ip>:<port> is down	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be down.
HC: backend <ip>:<port> is up again	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be up.
Host <host ip> has been down too long: is no longer accounted for in the license pool.	WARNING	AAA	The host has been down too long (more than 30 days) and is no longer accounted for in the license pool.
Host <host ip> is up: accounted for in the license pool.	INFO	AAA	A host that has been down too long is up again and is now sharing its licenses in the license pool.

Message	Severity	Type	Explanation
HSM mode: <mode>	INFO	Startup	Hardware Security Mode <mode>.
hsm_not_logged_in	ALARM (CRITICAL)	System Control	After a reboot, login to the HSM card is required.
hsm_tampered_with	ALARM (CRITICAL)	System Control	The HSM card has been tampered with.
html error: <reason>	ERROR	Traffic Processing	Error encountered when parsing HTML. Probably non-standard HTML.
http error: <reason>, Request="<method> <host><path>"	ERROR	Traffic Processing	A problem was encountered when parsing the HTTP traffic. This is either an indication of a non-standard client/ server or an indication that the AVG's HTTP parser has gotten out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.
http header warning cli: <reason> (<header>)	ERROR	Traffic Processing	The client sent a bad HTTP header.
http header warning srv: <reason> (<header>)	ERROR	Traffic Processing	The server sent a bad HTTP header.
HTTP NotLoggedIn Vpn="<id>" Host="<host>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	AAA	The remote user was not logged in to the specified web server requested from the Portal.
HTTP Rejected Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>"	INFO	AAA	The remote user failed to access the specified web server requested from the Portal.

Message	Severity	Type	Explanation
Request="<method> <host> <path>"			
HTTP Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	AAA	The remote user has successfully accessed the specified web server requested from the Portal.
Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>	ERROR	Traffic Processing	AVG received reply for non-configured DNS server.
Ignoring request to roam from %s to %s	WARNING	IPsec	Dropping roam request because old and new source IP are same.
Ignoring request to roam from %s to %s due to invalid source. Expecting %s	WARNING	IPsec	Dropping roam request message because mismatch in source in payload and header.
Ignoring unauthenticated informational message from %s	WARNING	IPsec	Dropping message without the authentication hash.
ike Connected successfully to erlang	INFO	IPsec	IKE daemon has started and connected to the registry database.
Ike not started due: No license	NOTICE	IPsec	If no licence can be found (such as on old ASA 310), IKE is not started.
internal error: <no>	ERROR	Traffic Processing	An internal error occurred. Contact support with as much information as possible to reproduce this message.
IPSec Mobility is disabled. Roaming request denied.	WARNING	IPsec	Dropping the roaming request, the

Message	Severity	Type	Explanation
			Mobility is disabled in configuration.
IPSec SA Established with %s, IPComp %s, inbound CPI 0x%x	INFO	IPsec	IPsec SA Established.
IPSEC server ~s uses default interface (interface ~p not configured)	WARNING	IPsec	This indicates possible badly configured default gateways on some Secure Service Partitioning interface.
IPSEC server <id> uses default interface (interface <n> not configured)	WARNING	Traffic Processing	A specific interface is configured to be used by the IPsec server but this interface is not configured on the VPN Gateway.
ISAKMP SA Established with %s	INFO	IPsec	ISAKMP SA Established.
isd_down	ALARM (CRITICAL)	System Control	A member of the AVG cluster is down. This alarm is only sent if the cluster contains more than one VPN Gateway.
javascript error: <reason> for: <host><path>	ERROR	Traffic Processing	JavaScript parsing error encountered when parsing content from <host><path>. This could be a problem in the AVG AVG JavaScript parser, but most likely a syntactical error in the JavaScript on that page.
jscript.encode error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing an encoded JavaScript. It may be a problem with the JavaScript parser in the AVG or it could be

Message	Severity	Type	Explanation
			a problem on the processed page.
LDAP backend(s) unreachable Vpn= \"<id>\" AuthId= \"<authid>\"	ERROR	AAA	Shown if LDAP server(s) cannot be reached when a user tries to login to the Portal.
license	ALARM (WARNING)	System Control	One or several VPN Gateways in the cluster do not have the same SSL VPN license (with reference to number of concurrent users).
license	ALARM (WARNING)	System Control	The (demo) license loaded to the local VPN Gateway expires within 7 days. Check loaded licenses using the **/cfg/sys/cur** command.
license_expire_soon	EVENT	System Control	Indicates that the loaded (demo) license at the <IP> VPN Gateway expires within 7 days.
license_expired	EVENT	System Control	Indicates that the demo license at host <IP> has expired. Check the loaded licenses with **/cfg/sys/cur**.
License expired	WARNING	Traffic Processing	The loaded (demo) license on the VPN Gateway has expired. The VPN Gateway now uses the default license.
Loaded <ip>:<port>	INFO	Startup	Initializing virtual server <ip>:<port>.
Loaded ca certificate %s	INFO	IPsec	Loaded CA certificate with name %s. This certificate is

Message	Severity	Type	Explanation
			used to verify client certificates.
Loaded server cert %s	INFO	IPsec	Loaded server certificate with name %s. This certificate must be signed by a trusted CA in the client.
Log off notif for non-existing session id %u	WARNING	IPsec	AAA notified about log-off for a non-existing session.
log_open_failed	ALARM (MAJOR)	System Control	The event log (where all events and alarms are stored) could not be opened.
Logs filesystem re-initialized	ERROR	OS	Loss of logs.
make_software_release_permanent_failed	ALARM (CRITICAL)	System Control	Failed to make a new software release permanent after being activated. The system will automatically revert to the previous version.
Malformed ADDRESS_CHANGE notify message received from %s	WARNING	IPsec	Dropping invalid ADDRESS_CHANGE (Mobility) request.
Message from %s dropped because SPI is not found	WARNING	IPsec	Dropping message because SPI is not found.
Missing files in config filesystem	ERROR	OS	Possible loss of configuration. Followed by the message "Config filesystem re-initialized - reinstall required" or "Config filesystem restored from backup".
No cert supplied by backend server	INFO	Traffic Processing	No certificate supplied by backend server when doing

Message	Severity	Type	Explanation
			SSL connect. Session terminated to backend server.
No CN supplied in server cert <subject>	INFO	Traffic Processing	No CN found in the subject of the certificate supplied by the backend server.
No IPsec encryption type selected for %s - terminating connection attempt	WARNING	IPsec	IPsec encryption does not match with the configured value.
No more than <nr> backend supported	INFO	Startup	Generated when more than the maximum allowed backend servers have been configured.
No PortalGuard license loaded: VPN <id> *will* use portal authentication	WARNING	Traffic Processing	The PortalGuard license has not been loaded on the VPN Gateway but **`/cfg/vpn # /server/portal/authenticate`** is set to off.
No response from %s for maximum retransmission attempts %d	INFO	IPsec	Maximum number of retransmission attempts reached.
No Secure Service Partitioning license loaded IPSEC server ~s *will not* use interface ~p	WARNING	IPsec	Secure Service Partitioning licence not loaded.
No Secure Service Partitioning loaded: server <id> *will not* use interface <n>	WARNING	Traffic Processing	The Secure Service Partitioning license has not been loaded on the VPN Gateway but the server is configured to use a specific interface.
No TPS license limit	INFO	Startup	Unlimited TPS license used.

Message	Severity	Type	Explanation
partitioned_network	EVENT	System Control	Sent to indicate that a VPN Gateway is recovering from a partitioned network situation.
PFS is required but not provided by %s	WARNING	IPsec	PFS (Perfect Forward Secrecy) is configured locally, but the peer does not provide it.
PORTAL Rejected Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user failed to access the specified folder/ directory on the specified file server requested from the Portal's Files tab.
PORTAL Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user has successfully accessed the specified folder/ directory on the specified file server requested from the Portal's Files tab.
Proxy connect host name too long: <host>	ERROR	Traffic Processing	The host name is too long to perform proxy connect. Make the host name shorter or remove the domain from the proxy connect mapping.
Quick mode initiation to %s failed, error - %s	WARNING	IPsec	Quickmode initiation failed.
Rebooting to revert to permanent OS version	ERROR	OS	Happens after "Config filesystem re-initialized - reinstall required" or "Config filesystem restored from backup" if software upgrade is in progress (i.e. if failure at first boot on new OS version).

Message	Severity	Type	Explanation
Received Delete IPSEC SA message from %s	INFO	IPsec	Received Delete IPsec SA message.
Received Delete ISAKMP SA message from %s	INFO	IPsec	Received Delete ISAKMP SA message.
reload cert config done	INFO	Config Reload	Certificate reloading done.
reload cert config start	INFO	Config Reload	Starting reloading of certificates.
reload configuration done	INFO	Config Reload	Virtual server configuration reloading done.
reload configuration network down	INFO	Config Reload	Accepting new sessions are temporarily put on hold.
reload configuration network up	INFO	Config Reload	Resuming accepting new sessions after loading new configuration.
reload configuration start	INFO	Config Reload	Virtual server configuration reloading start.
Restarting proxy due to <reason>	INFO	Traffic Processing	Traffic subsystem restarted due to <reason>.
Returned IP	INFO	IPsec	An IP address was returned to the IP address pool.
revocation byte length: %d	INFO	IPsec	Loading certificate revocation list of length %d.
Root filesystem corrupt	EMERG	OS	The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall to recover.
Root filesystem repaired - rebooting	ERROR	OS	fsck found and fixed errors. Probably OK.
Server <id> uses default interface	WARNING	Traffic Processing	A specific interface is configured to be used

Message	Severity	Type	Explanation
(interface <n> not configured)			by the server but this interface is not configured on the VPN Gateway.
Set CSWIFT as default	INFO	Startup	Using CSWIFT SSL hardware acceleration.
Shutting sslproxy down.	INFO	Traffic Processing	Traffic subsystem has been stopped.
Because we use clicerts, force adjust totalcache size to : <size> per server that use clicerts	INFO	Startup	Generated if the size of the SSL session cache has been modified.
single_master	ALARM (WARNING)	System Control	Only one master VPN Gateway in the cluster is up and running.
slave_not_starting	ALARM (WARNING)	System Control	The portal handling subsystem cannot be started.
socks error: <reason>	ERROR	Traffic Processing	Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.
SOCKS Rejected Vpn="<id>" User="<user>" SrcIP="<ip>" Request="<request>"	INFO	AAA	The remote user failed to perform an operation by using one of the features available under the Portal's Advanced tab.
socks request: socks version <version> rejected	ERROR	Traffic Processing	Socks request of version <version> received and rejected. Most likely a non-standard socks client.
SOCKS Vpn="<id>" User="<user>" SrcIP="<ip>"	INFO	AAA	The remote user has successfully performed an operation by using

Message	Severity	Type	Explanation
Request="<request>"			one of the features available under the Portal's Advanced tab.
software_configuration_changed	EVENT	System Control	Indicates that release <VSN> (version) has been <Status> (unpacked/installed/permanent).
software_release_copying	EVENT	System Control	Indicates that <IP> is copying the release <VSN> from another cluster member.
software_release_rebooting	EVENT	System Control	Indicates that a VPN Gateway (<IP>) is rebooting on a new release (i.e. a VPN Gateway that was not up and running during the normal installation is now catching up).
ssi_mipishere	EVENT	System Control	Tells that the MIP (management IP address) is now located at the VPN Gateway with the <IP> host IP address.
SSL connect failed: <reason>	ERROR	Traffic Processing	SSL connect to backend server failed with <reason>.
ssl_hw_fail	ALARM (MAJOR)	System Control	The SSL hardware acceleration card could not be found or initiated. This will cause the VPN Gateway to run with degraded performance.
Started ssl-proxy	INFO	Startup	Traffic subsystem started.
System started [isdssl-<version>]	INFO	System Control	Sent whenever the system control

Message	Severity	Type	Explanation
			process has been (re)started.
The private key and certificate don't match for <server nr>	ERROR	Traffic Processing	Key and certificate does not match for server #. The certificate has to be changed.
TPS license limit (<limit>) exceeded	WARNING	Traffic Processing	The transactions per second (TPS) limit has been exceeded.
TPS license limit: <limit>	INFO	Startup	TPS limit set to <limit>.
Unable to find client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Reconfigure.
Unable to use client certificate for <server #>	ERROR	Traffic Processing	Certificate for doing sslconnect is not valid. Reconfigure.
Unable to use client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Reconfigure.
Unable to use the certificate for <server nr>	ERROR	Traffic Processing	Unsuitable certificate configured for server #.
unknown WWW-Authenticate method, closing	ERROR	Traffic Processing	Backend server sent unknown HTTP authentication method.
Updating Ike profile %s	INFO	IPsec	A CLI/BBI change in IKE profile %s forces an update of the profile.
Using <hwtype> hardware	INFO	Startup	Using <hwtype> hardware for SSL acceleration.
Using new IKE. IKE Profile %s received in Auth Reply.	INFO	IPsec	Received new IKE profile from AAA (received from RADIUS).
vbscript error: <reason> for: <host><path>	ERROR	Traffic Processing	VBScript parsing error encountered when parsing content

Message	Severity	Type	Explanation
			from <host><path>. This could be a problem in the AVG AVG VBScript parser, but most likely a syntactical error in the VBScript on that page.
VPN AddressAssigned Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" TunIP="<inner tunnel ip>"	INFO	AAA	Source IP address for the connection between the VPN Gateway and the destination address (inner tunnel) has been allocated.
VPN LoginFailed Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" [User="<user>"] Error=<error>	INFO	AAA	Login to the VPN failed. The remote user's access method, client IP address and user name is shown.
VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>"	INFO	AAA	Login to the VPN succeeded. The remote user's access method, client IP address, user name and group membership is shown.
VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>" TunIP="<inner tunnel ip>"	INFO	AAA	Login to the VPN succeeded. The remote user's access method, client IP address, user name and group membership is shown as well as the IP address allocated to the connection between the VPN Gateway and the destination address (inner tunnel).

Message	Severity	Type	Explanation
VPN Logout Vpn="<id>" SrcIp="<ip>" User="<user>"	INFO	AAA	Remote user has logged out from the VPN.
www_authenticate: bad credentials	ERROR	Traffic Processing	The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.

Glossary

Access Rules	When a user tries to log in to the VPN, either through the Portal page or through a VPN client, his or her group membership determines the access rights to different servers and applications on the intranet. This is done by associating one or more access rules (each containing parameters such as allowed network, ports and paths) with a group.
ARP	Address Resolution Protocol. A network layer protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.
Base Profile	Refers to links and access rules specified for a user group directly under the Group level. If extended profiles are used, the base profile's links and access rules will be appended to the extended profile's links and access rules.
Branch Office Tunnel	Secure IPsec tunnel between two VPN Gateways (or cluster of VPN Gateways) or similar devices. The tunnel is automatically established when traffic destined for specific remote networks is detected, provided traffic was initiated from a network allowed to send traffic through the tunnel. BO tunnels can e.g. be set up between a main office and a branch office.
CA (Certificate Authority)	A trusted third-party organization or company that issues digital certificates. The role of the CA in this process is to guarantee that the entity granted the unique certificate is, in fact, who he or she claims to be.
CLI (Command Line Interface)	The text-based interface on the VPN Gateway, presented to the user after having logged in. The CLI can be accessed through a console connection or remote connection (Telnet or SSH). The CLI is used for collecting information and configuring the VPN Gateway.

Cluster (of AVGs)	A cluster is a group of VPN Gateways that share the same configuration parameters. There can be more than one AVG cluster in the network, each with its own set of parameters and services to be used with different real servers. Every cluster has a Management IP address (MIP), which is an IP alias to one of the master VPN Gateways in the cluster.
Console Connection	A connection to the VPN Gateway established through the console port.
CRL (Certificate Revocation List)-	A list containing the serial numbers of revoked client certificates. Each CA issues and maintains their own CRLs. If you generate client certificates on the VPN Gateway, you can also create your own CRL.
CSR (Certificate Signing Request)	A request for a digital certificate, sent to a CA. On the VPN Gateway, you can generate a CSR from the command line interface by using the request command.
DCE (Data Communications Equipment)	A device that communicates with a Data Terminal Equipment (DTE) in RS-232C communications.
DER (Distinguished Encoding Rules)	A process for unambiguously converting an object specified in ASN.1 (such as an X.509 certificate, for example) into binary values for storage or transmission on a network.
Digital Certificate	The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by trusted third parties known as certificate authorities (CAs), after verifying that a public key belongs to a certain owner. The certification process varies depending on the CA and the level of certification.
Digital Signature	A digital guarantee ensures that a document has not been altered, if it was carried in an electronically-sealed envelope. The “signature” is an encrypted digest of the text that is sent with the text message. The recipient decrypts the signature digest and also recomputes the digest from the received text. If the digests match, the message is proved intact and tamper free from the sender. A digital signature ensures that the document originated with the person signing it and that it was not tampered with after the signature was applied. However, the sender could still be an impersonator and not the person he or she claims to be. To verify that the message was indeed sent by the person

	claiming to send it requires a digital certificate (digital ID) which is issued by a certification authority.
DIP (Destination IP) Address	The destination IP address of a frame.
DPort (Destination Port)	The destination port number, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.
DTE (Data Terminal Equipment)	A device that controls data flowing to or from a computer. The term is most often used in reference to serial communications defined by the RS-232C standard. This standard defines the two ends of the communication channel as being a DTE and DCE device. However, using a null-modem cable, a DTE to DTE communication channel can also be established between, for example, two computers.
Extended Profile	Extended profiles can be defined for a user group if other links and access rules should apply when the user authenticates by means of a specific authentication method or when connecting from a specific IP address or network.
HTTP Proxy	Java applet accessible on the Portal page's Advanced tab, enabling links executed on complex intranet Web pages (containing plugins like Flash, Shockwave and Java applets) to be sent through a secure connection to the SSL server for redirection.
Master	A VPN Gateway in a cluster that is in control of the MIP address, or can take over the control of the MIP address should another master fail. Configuration changes in the cluster are propagated to other members through the master VPN Gateways.
MIB (Management Information Base)	An SNMP structure that describes which groups and objects that can be monitored on a particular device.
MIP (Management IP)	An IP address that is an IP alias to a master VPN Gateway in a cluster of VPN Gateways. The MIP address identifies the cluster and is used when making configuration changes through a Telnet or SSH connection or through the Browser-Based Management Interface (BBI).
Net Direct Client	The Net Direct client is an SSL VPN client that can be downloaded from the Portal for each user session. As opposed to the LSP and TDI versions of the SSL VPN client, the Net Direct client does

	not have a user interface. Another difference is that the Net Direct client is packet-based, while the SSL VPN clients uses system calls. The packet-based solution supports more applications (e.g. Microsoft Outlook).
Nslookup	A utility used to find the IP address or host name of a machine on a network. To use the nslookup command on the VPN Gateway, it must have been configured to use a DNS server.
NTP (Network Time Protocol)	A protocol used to synchronize the real-time clock in a computer. There are numerous primary and secondary servers on the Internet that are synchronized to the Coordinated Universal Time (UTC) through radio, satellite, or modem.
AVG	Avaya VPN Gateway.
Passphrase	Passphrases differ from passwords only in length. Passwords are usually short, from six to ten characters. Short passwords may be adequate for logging onto computer systems that are programmed to detect a large number of incorrect guesses, but they are not safe for use with encryption systems. Passphrases are usually much longer—up to 100 characters or more. Their greater length makes passphrases more secure.
PEM (Privacy Enhanced Mail)	A standard for secure e-mail on the Internet. It supports encryption, digital signatures, and digital certificates as well as both private and public key methods. Keys and certificates are often stored in the PEM format.
Ping (Packet INternet Groper)	A utility used to determine whether a particular IP address is online.
PKCS #12	A standard for storing private keys and certificates.
PKI (public key infrastructure)	Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread. A PKI is also called a trust hierarchy.
Portal	The Portal Web page is displayed following a successful login to a VPN server of the portal type.

	The Portal contains different tabs from where the user can access various intranet resources such as Web, mail, and file servers.
Portal Guard	The Portal Guard feature is an easy way of “converting” an existing HTTP site to generate HTTPS links, secure cookies etc. The VPN Gateway will not only handle the SSL processing but also see to it that all existing Web links are rewritten to HTTPS. This eliminates the need to rewrite each link manually.
Port Forwarder	Java applet accessible on the Portal page’s Advanced tab, enabling transparent access to applications through a secure connection. By specifying an arbitrary port number on the client along with the desired intranet host and port number, the user can access an intranet application by connecting to localhost on the specified port number.
Secure Service Partitioning	Feature designed to partition a cluster of VPN Gateways into separate VPNs. The idea is to give service providers (ISPs) the possibility to host multiple VPN customers on a shared Remote Access Services (RAS) platform.
Setup Utility	When turning on a VPN Gateway the very first time, the Setup utility starts up automatically. The Setup utility is used for performing a basic configuration of the VPN Gateway. The Setup utility first presents you with the choice of setting up the AVG as a single device, or to add the VPN Gateway to an existing cluster. If you perform a reinstallation of the AVG software, you must also enter the Setup Utility after the VPN Gateway has rebooted.
SIP (Source IP) Address	The source IP address of a frame.
Slave	A VPN Gateway that depends on a master VPN Gateway in the same cluster for proper configuration.
SNMP (Simple Network Management Protocol)	A network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (a VPN Gateway, for example), to the workstation console (or SNMP manager) used to oversee the network. The SNMP agents return information contained in a MIB (Management Information Base), which is a data

	structure that defines what information is obtainable from the device.
SOCKS	A generic, proxy protocol for TCP/IP-based networking applications. The SOCKS protocol provides a flexible framework for developing secure communications by easily integrating other security technologies, for example, SSL. SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS server, without requiring direct IP reachability.
SPO (Secure Portable Office)	Secure Portable Office client is the proprietary VPN client that resides on portable PC compatible memory devices.
SPort (Source Port)	The source destination port, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.
SSH (Secure Shell)	A program used to log into another computer over a network, execute commands in a remote machine, and move files from one machine to another. SSH provides strong authentication and secure communications over insecure channels.
SSL (Secure Sockets Layer) Protocol	The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and following higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.
SSL VPN client	Windows application with SOCKS support. When installed on a user's computer, transparent access (not through the Portal page) to intranet applications is enabled.
TLS (Transport Layer Security)	The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Traceroute	A utility used to identify the route used for station-to-station connectivity across the network.

Trap	If a trap is defined in the MIB, a trap message is sent from the SNMP agent to the SNMP manager when the trap is triggered. A trap can for example define a hardware failure in a monitored device.
TunnelGuard	TunnelGuard is an application that checks that the required components (executables, DLLs, configuration files, etc.) are installed and active on the remote user's machine.
URI (Uniform Resource Identifier)	The addressing technology from which URLs are created. Technically, URLs such as HTTP:// and FTP:// are specific subsets of URLs, although the term URL is mostly heard.
VIP (Virtual IP) Address	An IP address that the remote user should connect to access Portal/VPN (in clientless mode) or simply the VPN (in transparent mode).
Virtual SSL Server	A virtual SSL server handles a specific service on the VPN Gateway, such as HTTPS, SMTPS, IMAPS, or POP3S. You can create up to 256 virtual SSL servers per AVG cluster. To authenticate itself towards clients making requests for the specified service, the virtual SSL server is configured to use a digital certificate.
VLAN (Virtual Local Area Network)	VLANs are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.
X.509	A widely-used specification for digital certificates that has been a recommendation of the ITU since 1988.
X11 Forwarding	The X Window System (commonly X11 or X) is a windowing system for bitmap displays. It is the standard toolkit and protocol to build graphical user interfaces on Unix, Unix-like operating systems and OpenVMS, and is available for almost all modern operating systems. The VPN Gateway supports secure display of X11 across the Internet by way of X11 Forwarding, supported by the SSH applet on the Portal's Advanced tab and the Terminal link type.

Glossary

Index

S