Avaya IP Office SSL VPN Solutions Guide

Release 9.0
Issue 02.01
September 2013

© 2013 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

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

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

License types

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

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

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

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

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

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

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

installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Document changes since last issue 7
Chapter 2: About the SSL VPN service 9
Deployment options 9
Operating modes 10
System architecture 13
System requirements and limitations 15
Related documentation 16
Chapter 3: Workflow for configuring an SSL VPN 17
Chapter 4: Configuring the Avaya VPN Gateway 19
Initial planning and setup 19
Configuring the Avaya VPN Gateway procedures 20
Basic AVG configuration 22
Enabling remote access services 23
Running the Net Direct Wizard 23
Modifying the default AVG for SSL VPN 24
Configuring local authentication 25
Configuring RADIUS authentication 26
RADIUS server configuration attributes 29
Chapter 5: Configuring an SSL VPN for Avaya support 33
Configuring an SSL VPN using an on-boarding file 33
Using the on-boarding file to modify an existing service 34
Chapter 6: Configuring an SSL VPN for Avaya partner support 37
Configuring the SSL VPN service 39
Installing a certificate 41
Configuring short codes 42
Configuring a short code to enable the SSL VPN service 43
Configuring a short code to disable the SSL VPN service 43
Configuring an auto attendant 44
Configuring alarm notifications 46
Configuring SNMP trap destinations 47
Configuring email alarm notifications 48
Configuring syslog entries 49
Configuring a static route 50
Chapter 7: Network address and port translation (NAPT) rules 51
Configuring NAPT rules 51
Deleting an NAPT rule 52
Chapter 8: Verify the connection between IP Office and AVG 53
Verifying the connection using SysMonitor 53
Verifying the AVG SSL VPN deployment using System Status Application 54
Verifying the connection using the AVG BBI 54
Sending a test alarm 54
Chapter 9: Monitoring and managing the IP Office system 57
Monitoring IP Office remotely using SSA 58
Monitoring IP Office remotely using SysMonitor 59

Remotely monitoring LAN devices using the SSL VPN tunnel 59
Configuring IP Office remotely using Web Manager 60
Configuring IP Office remotely using Manager 61
Configuring Server Edition systems remotely using IP Office Manager for Server Edition 62
Configuring Server Edition systems remotely using Web Control 63
Chapter 9: Upgrading IP Office remotely 67
Chapter 10: Monitoring the SSL VPN service 69
Viewing the tunnel status 69
Tunnel status field descriptions: summary table 70
Tunnel status field descriptions: detail table 70
Monitoring alarms using SSA 72
SSA alarm descriptions 73
Troubleshooting the SSL VPN service 74
SysMonitor output descriptions 74
Chapter 11: Maintaining the SSL VPN service 77
Enabling and disabling the service 77
Enabling the service using Manager 78
Disabling the service using Manager 79
Enabling the service using SSA 79
Disabling the service using SSA 80
Enabling the service using a short code 80
Disabling the service using a short code 81
Enabling and disabling the service using set-based administration 81
Enabling and disabling the service using programmable keys 82
Resetting the password 83
Resetting the password using an on-boarding file 83
Resetting the password using Manager 84
Chapter 12: Appendix A: AVG Quick Setup log file example 87
Chapter 13: Appendix B: Modifying the default AVG for SSL VPN (with screens) 89
Chapter 14: Appendix C: Configuring RADIUS authentication (with screens) 95
Chapter 15: Appendix D: AVG configuration settings 101
Index 111

Chapter 1: Document changes since last issue

The following changes have been made to this document for IP Office release 8.7.

Network Address and Port Translation (NAPT)

Network Address and Port Translation (NAPT) was a new feature in the 8.1 Feature Pack release. NAPT rules allow a support service provider to establish a remote connection to a LAN device on a private IP Office network. See Network address and port translation (NAPT) rules on page 51.

In release 8.7, NAPT is supported on Server Edition systems.

Document changes since last issue

Comments? infodev@avaya.com

Chapter 2: About the SSL VPN service

The IP Office SSL-VPN remote access solution is a fast and easy way to set up a secure remote access at broadband speeds. The solution is designed to provide Avaya and Avaya partners with reliable remote access that enhances service delivery while reducing the cost associated with providing onsite services. The solution enables partners of any size, to create an infrastructure that automates management and maintenance of IP Office systems.

Services provided by SSL VPN

The SSL VPN service provides secure tunneling between the Avaya IP Office hardware installed at a customer site and an Avaya VPN Gateway (AVG) installed at a service provider site. This secure tunnel allows service providers to offer remote management services to customers, such as fault management, monitoring, and administration. It provides administrators with the ability to:

- forward traffic over the SSL VPN service using split tunneling routes and static routes
- remotely monitor IP Office over SSL VPN service connected to an AVG server using System Status Application (SSA) or SysMonitor
- remotely manage IP Office systems using Avaya IP Office Manager or IP Office Manager for Server Edition
- receive SNMP traps, syslog entries, and SMTP email alarms from IP Office over an SSL VPN service connected to an AVG server
- enable and disable the tunnel using Manager or IP Office Manager for Server Edition
- enable and disable the tunnel using short codes, auto-attendant, or set-based administration
- run multiple instances of SSL VPN service concurrently

Deployment options

Avaya remote support services

The SSL VPN solution is an integral element of the IP Office Support Services (IPOSS), allowing Avaya to provide industry leading remote troubleshooting and technical support. Establishing the SSL VPN connection to Avaya is greatly simplified by the automated on-boarding capability. The on-boarding process includes inventory extraction, registration into GRT to create the installed base record, and technical registration for the remote connectivity to Avaya.

For additional details on the IPOSS maintenance offer, go to the IP Office Support Services page on the Avaya Sales Portal.

Remote support services provided by Avaya partners

Separate from the IPOSS offer, partners have the option to leverage the SSL VPN client delivered in IP Office R8.1, in combination with the Avaya VPN gateway (AVG) solution, to

create their own SSL VPN infrastructure. This document provides information and procedures to assist those Avaya partners who want to establish their own SSL VPN solution for remote access, as part of their maintenance support to their customers.

The partner configured SSL VPN solution is supported on Standard Edition and Server Edition IP Office systems.

Operating modes

Operating modes

The SSL VPN service is supported on IP500v2 hardware. The IP500 control module is not supported.

The SSL VPN is supported with IP Office operating in the following modes. Branch mode is not supported.

- IP Office Standard Edition (Essential, Advanced, and Preferred modes)
- Server Edition
  - Server Edition Primary
  - Server Edition Secondary
- Server Edition Expansion System
  - Server Edition Expansion System (V2), an IP500v2 expansion system
  - Server Edition Expansion System (L), a Linux expansion system
- Basic Edition

Note:

Basic Edition is only supported on deployments using Avaya IP Office Support Services (IPOSS). Basic Edition is not supported with an SSL VPN deployed for Avaya partner support services.

Supported features

The functionality available depends on the operating mode you are using. This section provides an overview of the SSL VPN functionality and lists the functions available in each mode.

Supported features	Operating mode			
	Standard Edition	Server Edition	Server Edition Expansion System	Basic Edition
Connectivity				

Supported features	Operating mode			
	Standard Edition	Server Edition	Server Edition Expansion System	Basic Edition
Always-on SSL VPN connection to an AVG server	✔	✔	✔	✔
Split tunneling routes	✔	✔	✔	✔
Static routes	✔	✔	✔	✔
Multiple instances of SSL VPN service running concurrently	✔	✔	✔	✔
LAN device access (NAPT)	✔	✔	✔	—
Fault management				
Generate SNMP traps	✔	✔	✔	✔
Generate syslog entries	✔	✔	✔	—
Generate email notifications for alarms	✔	✔	✔	—
Generate test alarms	✔	✔	✔	✔
Monitoring and administration				
Remote management using Manager or IP Office Manager for Server Edition	✔	✔	✔	✔
Remote monitoring using System Status Application	✔	✔	✔	✔
Remote monitoring using SysMonitor	✔	✔	✔	✔
Enable and disable the SSL VPN service through shortcodes	✔	✔	✔	—

Supported features	Operating mode			
	Standard Edition	Server Edition	Server Edition Expansion System	Basic Edition
Enable and disable the SSL VPN service through set-based menus	—	—	—	✔
Enable and disable the SSL VPN service through Manager or IP Office Manager for Server Edition	✔	✔	✔	—
Enable and disable the SSL VPN service using auto-attendant	✔	✔	✔	—
Enable and disable the SSL VPN service using programmable keys on Avaya deskphones	✔	✔	✔	✔
Remote upgrade of IP Office to new releases	✔	✔	✔	✔

Monitoring and administration tools

When the SSL VPN service is connected, you can manage and monitor the IP Office system remotely through the tunnel.

You can use the following tools to manage, upgrade, and configure the IP system remotely:

- IP Office Manager: An administrative application that allows you to configure system settings for IP Office Essential Edition systems.
  - IP Office Manager for Server Edition: When you launch IP Office Manager, you can choose to open a configuration using IP Office Manager for Server Edition mode. This mode allows you to administer Server Edition servers and expansion systems.
- IP Office Basic Edition – Web Manager: a browser-based tool that allows you to configure system settings for IP Office.

You can use the following tools to monitor the IP Office system remotely:

- System Status Application (SSA): The System Status Application is a diagnostic tool that you can use to monitor the status of IP Office systems. SSA reports real-time and historical events as well as status and configuration data.
- SysMonitor: The SysMonitor application displays operating information about the IP Office system. It can capture the information to log files for analysis.

System architecture

The SSL VPN service provides secure tunneling between the IP Office hardware installed at a customer site and an Avaya VPN Gateway (AVG) installed at a service provider site. Use the information in this section to understand the network architecture used by the SSL VPN service.

Network interface cards

Avaya recommends that you deploy the AVG server in a two armed configuration with two network interface cards (NICs). One interface handles private traffic between the SSL VPN and the trusted intranet. This connection allows the SSL VPN service to access internal resources and allows you to configure and manage the IP Office system from a management station. The second interface handles traffic to and from the internet.

Routing

At the service provider site, you can configure corporate routing between the AVG and its private network. At the customer site, you can locate each IP Office system on the private side of a corporate router. The corporate router does not require configuration changes for the SSL VPN service to work.

IP Office forwards data to the AVG over the SSL VPN service using split tunneling routes or static routes. You must use one of these options to send traffic through the SSL VPN tunnel:

- let IP Office dynamically install split tunneling routes when the SSL VPN service connects with AVG, and remove these routes when the service disconnects
- configure a static route in IP Office Manager

Split tunneling:

When you install and configure AVG, you can add split network subnets or host addresses for a group. The IP Office system learns the routing information for the tunnel dynamically when the SSL VPN service successfully connects with the AVG. The split networks routes are removed when the SSL VPN service disconnects from AVG.

For information about configuring split tunneling on the AVG using Net Direct, see the *Avaya VPN Gateway Administration Guide* (NN46120-105) and the *Avaya VPN Gateway BBI Application Guide* (NN46120-102). For information about configuring split tunneling using the command line interface, see *CLI Application Guide* (NN46120-101).

Static routes:

As an alternative to split tunneling, you can configure a static route directly on the IP Office system. When you configure a static route, the system uses the IP route information configured in Manager to determine the destination for forwarded traffic. You must define the SSL VPN service as the destination.

Use a static route when:

- split tunneling routes are not advertised by the AVG and you need to send traffic through the tunnel
- the SSL VPN service is not connected to the AVG and you want to queue traffic to be forwarded through the tunnel when the connection is restored; in this case, IP Office temporarily queues a small number of packets that trigger the connection when the SSL VPN is in-service but disconnected

You can configure multiple static routes on the IP Office system.

Authentication

Each IP Office system can support multiple SSL VPN tunnels. Each instance of an SSL VPN service is assigned a unique private static IP address. When you connect the SSL VPN service, the AVG authenticates the IP Office system. For a small number of IP Office systems, you can use the Avaya VPN Gateway (AVG) local database to create user data needed for authentication. For larger deployments, it is recommended that you use a RADIUS server for authentication.

Service agent access

Service agents located at the service provider site can connect to any IP Office system that has an in-service SSL VPN connection to AVG. They can monitor and manage the IP Office system remotely by contacting the IP address of the SSL VPN tunnel, and can access the IP addresses of multiple SSL VPN services concurrently.

The AVG ensures SSL VPN tunnels cannot communicate with one another. You do not need to configure additional settings to ensure that tunnels remain secure and independent.

Fault management

A fault management server is an optional component in the SSL VPN service. Deploy a fault management server at the service provider site and use the SSL VPN service to send system faults to that server. You can set event filters to determine which faults are reported. For example, you can set filters to report any events related to the operation of the IP Office system, and you can also report faults that are specific to the operation of the SSL VPN service.

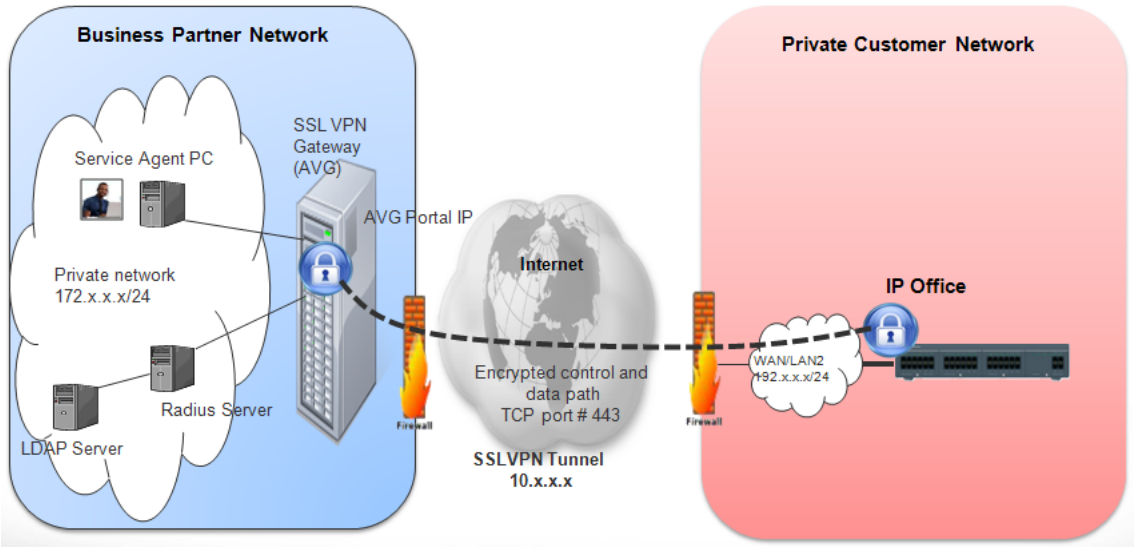
Avaya recommends that you set the SSL VPN service Account Name to match the SNMP Agent Device ID name. The SNMP Agent Device ID is configured in IP Office Manager on the **System** form, under **System Events**, **Configuration**.

Firewall traversal

The SSL VPN service works transparently through the firewall. You do not need to configure your corporate router to allow the SSL VPN service if you have already configured it for HTTPS traffic. The SSL VPN service uses the same destination port for its TCP traffic.

Architecture example

The following diagram shows an example of the architecture used by the SSL VPN service.



System requirements and limitations

Requirements

Bandwidth:

Ensure that the upload bandwidth is at least 90 kB/s (720 kb/s) with latency no greater than 150 ms (round trip). This specification ensures that Avaya Global Services can provide remote support through the SSL VPN service.

Authentication:

- For a small number of IP Office systems, you can use the Avaya VPN Gateway (AVG) local database to create user data needed for authentication.
- Large deployments require a RADIUS server. Avaya recommends that you use the Avaya Identity Engines Ignition Server as the RADIUS server.
- The IP Office system uses digital certificates to verify the identity of the AVG at end of the SSL VPN tunnel. You must configure certificates in AVG, and you must install the necessary X.509 certificates in the IP Office certificate store.

Licensing:

The SSL VPN Service does not require a license key.

Limitations

Small Community Networks:

If you deploy IP Office systems in a Small Community Network (SCN), you can configure an SSL VPN service between specific nodes in the SCN and the AVG. You cannot use the SSL VPN connection to remotely access other nodes in the SCN topology: the SSL VPN service

communicates only with the IP Office system that is its endpoint. You must configure an SSL VPN service for each node in the SCN that you want to access remotely.

Certificates:

You can store a maximum of 25 certificates in the IP Office trusted certificate store.

HTTP version:

If you use a browser with HTTP version newer than 1.1, you may be unable to connect to a LAN device using SSL VPN NAPT. If you have difficulty connecting to a LAN device, change your browser settings to use HTML version 1.1.

Related documentation

To install, configure, and administer the SSL VPN solution, you need to refer to the documentation for the Avaya IP Office system, the Avaya VPN Gateway (AVG), and the Avaya Identity Engines Ignition Server. In addition, you need to refer to the documentation provided by other vendors to support the hardware and software used in your network infrastructure.

Have the following Avaya documentation available to support the SSL VPN solution.

Avaya VPN Gateway documentation

- *Avaya VMware Getting Started Guide - Avaya VPN Gateway* (NN46120-302)
- *Avaya VPN Gateway User Guide* (NN46120-104)
- *Avaya VPN Gateway Administration Guide* (NN46120-105)
- *Avaya VPN Gateway BBI Application Guide* (NN46120-102)
- *Avaya VPN Gateway CLI Application Guide* (NN46120-101)

Avaya IP Office documentation

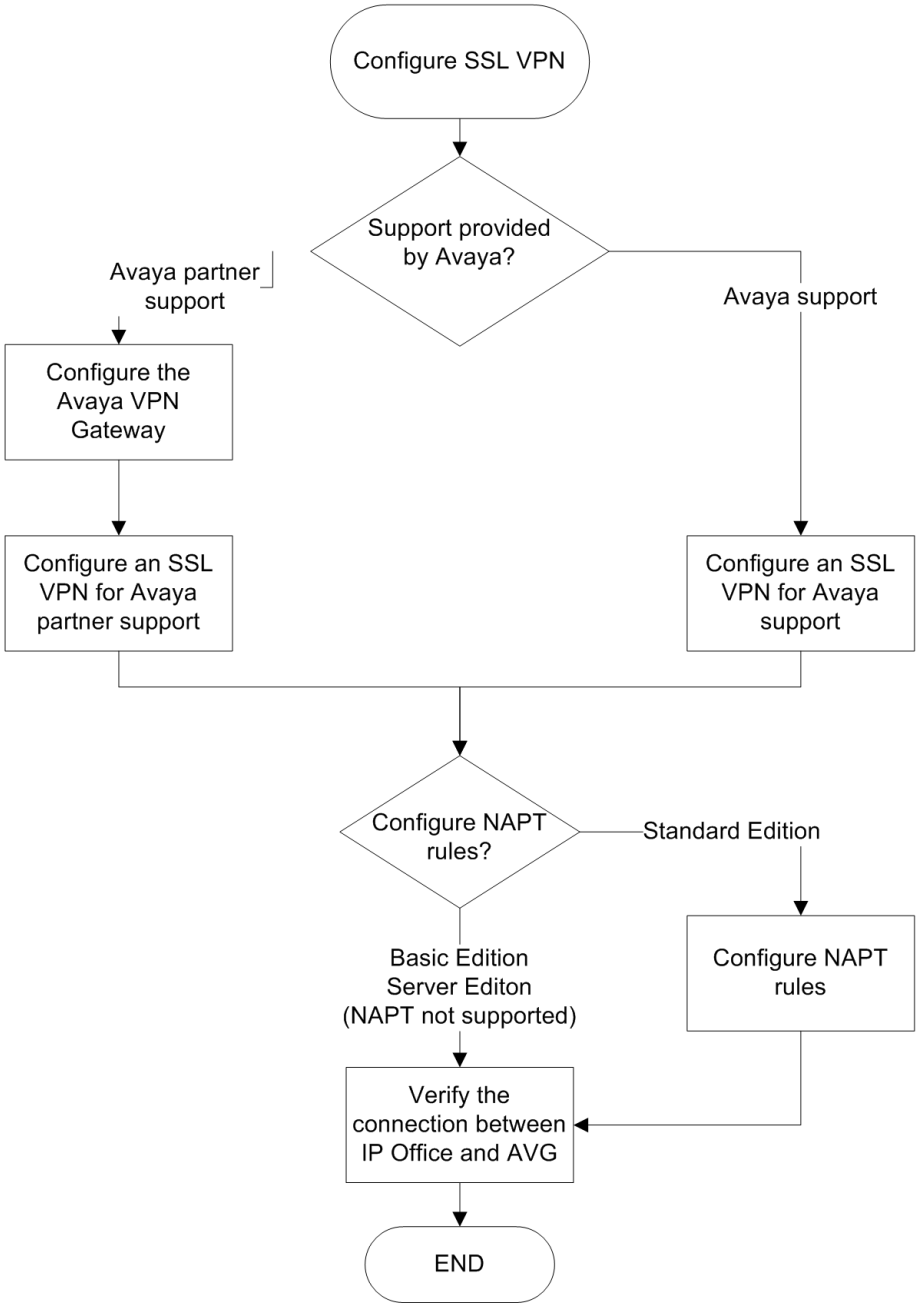
- *Avaya IP Office Basic Edition – Web Manager*
- *Avaya IP Office Manager*
- *Voicemail Pro Administration*
- *Embedded Voicemail Installation Guide*

Avaya Identity Engines Ignition Server documentation

- *Avaya Identity Engines Ignition Server — Configuration Guide* (NN47280-500)

Chapter 3: Workflow for configuring an SSL VPN

This work flow on the following page shows the sequence of tasks you perform to configure an SSL VPN.



Navigation

- Configuring the on page 19
- Configuring an SSL VPN for Avaya support on page 33
- Configuring an SSL VPN for Avaya partner support on page 37
- Network address and port translation (NAPT) rules on page 51
- Verify the connection between and on page 53

Chapter 4: Configuring the Avaya VPN Gateway

In order to provide support services with the SSL VPN solution, Avaya partners must configure the Avaya VPN Gateway (AVG)

This section provides information about the tasks that you must complete when you install and configure an AVG to support an SSL VPN connection with an IP Office system.

Before you configure the IP Office system for an SSL VPN service, you must configure the infrastructure that the service connects to. This section covers configuring the interoperation of the AVG with an IP Office system. To complete these tasks, you need to refer to the documentation suite for the AVG, as well as to the documentation provided by other vendors to support the hardware and software used in your network infrastructure.

The main tasks required for Avaya VPN Gateway deployment are described in this chapter. These are general recommendations. Exact deployment details may vary depending on the specific environment of the business partner.

Initial planning and setup

Virtualized environment

The SSL VPN client requires the Avaya VPN Gateway (AVG) installed in a virtualized environment as the VPN Gateway server. The only supported virtual environments are ESX and ESXi servers. There are three models of the AVG: 3050–VM, 3070–VM, and 3090–VM. For the hardware specifications for each model, see *VMware Getting Started Guide, Avaya VPN Gateway* (NN46120-302). You can download the complete AVG document collection from http://support.avaya.com.

Additional information on VMware ESXi servers is available from http://www.vmware.com.

Two arm configuration

Install the Avaya VPN Gateway (AVG) in a two arm configuration. This means that the AVG server must be equipped with two network interface cards (NIC). Assign a static IP address to each NIC.

- One interface handles private traffic and is used as a management interface.
- The second interface handles internet access and SSL VPN tunneling.

AVG software

There are two options for deploying the AVG software.

- Deploy AVG OVF virtual appliances
- Auto-installation CDROM

For AVG installation information and procedures, see *VMware Getting Started Guide, Avaya VPN Gateway* (NN46120-302).

Service Agent PC

Install the Service Agent (SA) PC on the private network and set the default gateway to the Avaya VPN Gateway (AVG) host IP address.

From the service agent PC

- The management interface IP (MIP) address is used to launch a Management Browser Based Interface (BBI) or a Command Line Interface (CLI) to configure and monitor the AVG.
- The SSL VPN tunneling IP address is used to remotely manage and monitor IP Office systems.

Configuring the Avaya VPN Gateway procedures

This task flow shows you the sequence of procedures you perform to configure the AVG.

Configure the Avaya VPN Gateway
Basic AVG configuration
Enable remote access service
Run the Net Direct wizard
Modify the default AVG
Configure RADIUS authentication?
No
Yes
Configure local authentication
Configure RADIUS authentication
RADIUS server configuration attributes
Test AVG SSL VPN deployment
END

Navigation

- Basic AVG configuration on page 22
- Enabling remote access services on page 23
- Running the Net Direct Wizard on page 23
- Modifying the default AVG for SSL VPN on page 24
- Appendix B Modifying the default AVG for SSL VPN (with screens) on page 89
- Configuring RADIUS authentication on page 26
- RADIUS server configuration attributes on page 29

Basic AVG configuration

Configuring the AVG from the service agent PC

When you start the VPN Gateway the first time, you will enter the **Setup** menu. This menu contains the **new** CLI command. This is a CLI based, intuitive, initial configuration wizard for the AVG that provides default settings to quickly bring up SSL connections from IP Office. It is useful for initial configuration and testing. This is the fastest way to initially configure AVG. Subsequently, the Browser-Based Management Interface (BBI) can be used to make changes recommended for SSL VPN connectivity. For more information see *User Guide Avaya VPN Gateway* (NN46120-104).

After using the new command to run the Quick Setup Wizard, the following settings have been created:

- A VPN. The VPN is typically defined for access to an intranet, parts of an intranet or to an extranet.
- A virtual SSL server of the portal type. A portal IP address is assigned to it, to which the remote user should connect to access the Portal. If you chose to use the VPN feature without an Application Switch, the portal server is set to standalone mode.
- A test certificate has been installed and mapped to the portal server.
- The authentication method is set to Local database and you have one test user configured. The test user belongs to a group called `trusted` whose access rules allow access to all networks, services and paths.
- One or several domain names are added to the DNS search list, which means that the remote user can enter a short name in the Portal's various address fields (for example, inside instead of inside.example.com if example.com is added to the search list).
- If you chose to enable HTTP to HTTPS redirection, an additional server of the HTTP type was created to redirect requests made with HTTP to HTTPS, because the portal server requires an SSL connection.

A printout of example configuration settings from the Quick Setup log file is available at Appendix A AVG Quick Setup log file example on page 87.

Enabling remote access services

Besides using the local VM console to configure VPN, the administrator also needs to manage the VPN by using a TELNET or SSH session or through the BBI. To allow VPN gateway remote configuration, the remote access services must be enabled.

Perform this procedure using the Command Line Interface (CLI). See the following AVG documents:

- *Command Reference Avaya VPN Gateway*
- *CLI Application Guide Avaya VPN Gateway*

Procedure

1. Log in to the AVG.
2. Enter the following commands.

```
/cfg/sys/adm/.
        telnet on
        ssh on
/cfg/sys/adm/https/.
        cert 1
        ena true
/cfg/sys/adm/http/.
        ena true
apply
```

Running the Net Direct Wizard

The Net Direct wizard lets you create a link on the Portal that downloads and launches a slim version of the Avaya VPN Client -- the Net Direct client. Run the Net Direct wizard from the Browser Based Manager Interface (BBI). See *Avaya VPN Gateway BBI Application Guide*.

Procedure

1. Log in to the AVG BBI.
   In the navigation pane on the left, select **Wizards**.
2. Click **Net Direct Wizard**.
3. On the **Net Direct settings for the selected VPN** page, select the **Enable Net Direct for this VPN** radio button.

4. On the **Default IP Pool Settings** page:
   - For **Default IPPool**, select **Local_pool**.
   - Enter the lower and upper IP addresses for the pool range.

Modifying the default AVG for SSL VPN

After running the Quick Setup and Net Direct configuration wizards, the default configuration must be modified to support an SSL VPN connection with an IP Office system.

Perform this procedure using the AVG browser-based interface (BBI). See *Avaya VPN Gateway BBI Application Guide*.

This procedure is duplicated in Appendix B Modifying the default AVG for SSL VPN (with screens) on page 89. This version of the procedure includes screen captures of the user interface.

Before you begin

Ensure that the default gateway configured on AVG responds to ICMP requests. If the default gateway does not respond to ICMP requests, the AVG cannot provide VPN services.

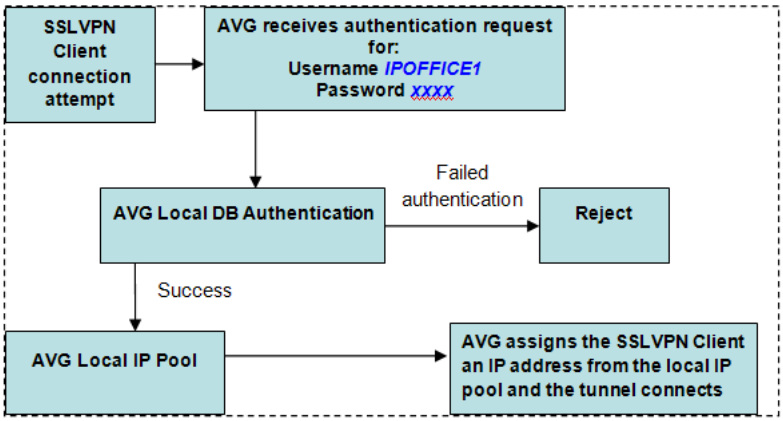
Procedure

1. Log on to the AVG BBI as administrator.
2. In the navigation pane on the left, select the **Config** tab and then **VPN Gateway** > **VPN1** > **IP Pool**.
3. The default VPN from the basic AVG configuration may already have a local pool. If not, you must add a local pool to the default VPN. On the **Add new IP Address Pool** page, add a local pool to the default VPN.
4. On the **Modify IP Address Pool** page, verify that the values in the **Lower IP** and **Upper IP** fields match values set using the Net Direct Configuration wizard.
5. On the **IP Pool** > **Network Attributes Settings** page, select the **Network Attributes** tab and enter the values for your network.
6. On the **IP Pool** page, set the **Default IP Pool** to the local pool created in step 3.
7. On the **Net Direct Client Access Settings** page, verify the settings created by the Net Direct Configuration wizard.
   - Ensure that **Idle Check** is set to **off**.
   - Ensure that the Net Direct Banner is set.

8. Set the portal link for launching the Net Direct client. On the **Portal Linkset Configuration** page, Select the **Portal Link** tab. In the **Link Type** field, select **Net Direct**.
9. On the **Networks for Split Tunnels** page:
    - set **Split Tunnel Mode** to **enabled**
    - set the split tunneling routes to reach the service agent on the private network
10. For VPN1, go to the groups page and select **Group1**. On the **Modify a Group** page, set the IP Pool to the local pool created in step 3.
11. Go to the **VPN1** > **Group1** > **Access Lists** page. On the **Firewall Access List** page, create an access rule if it was not created by default.
12. Go to the **VPN1** > **SSL** page. On the **Server Settings** page, under **SSL Settings** set **Ciphers** to **AES256-SHA** for a strong encryption.
13. Go to the **VPN1** > **Authorization** > **Services** page. Remove all the services set in the default configuration as they are not required by SSL VPN.
14. Go to the **VPN1** > **Authorization** > **Networks** page. Set the authorization network subnet that is referenced in one of the access rules that is set under **VPN1** > **Group1** > **Access Lists**.
15. Go to the **VPN1** > **General Settings** > **Session** page. Set **Session Idle Time** to 2 minutes.

Configuring local authentication

For a small number of IP Office systems, you can use the Avaya VPN Gateway (AVG) local database to create user data needed for authentication. This is a quick way to set up authentication when no external RADIUS authentication servers are available. Configure an IP Pool to dynamically assign IP addresses to the local users. The figure below shows the SSL VPN Client authentication flow and how the IP pool address allocation is done.



This procedure covers the manual steps to configure local authentication. Alternatively, you can configure authentication using the AVG authentication wizard.

Procedure

1. For **VPN1**, go to the **IP Pool Configuration** page and add a local IP pool.
2. Go to **VPN1** > **IP Pool** > **Add/Modify**. Set the IP pool dynamic range by entering values in the **Lower IP** and **Upper IP** fields.
3. Go to **VPN1** > **IP Pool** > **Network Attribute**. Set the **Client Netmask**.
4. On the **Add a Group** page, add a new group to VPN1.
5. Go to **VPN1** > **<Group_Name>** > **Modify Group**. Select the **General** tab and assign a local pool to the group by selecting it in the **IP Pool** field.
6. Select the **Access Lists** tab and specify the access list for the local users group.
7. Select the **Linksets** tab and assign the linksets.
8. Edit the VPN authentication settings. On the **Authentication Servers** page, add a new authentication server.
9. Go to **VPN1** > **<Auth_Server_Name>** > **Add/Modify Users** and add users to the group.
10. Edit the authentication server and specify the **Authentication Order**.

Configuring RADIUS authentication

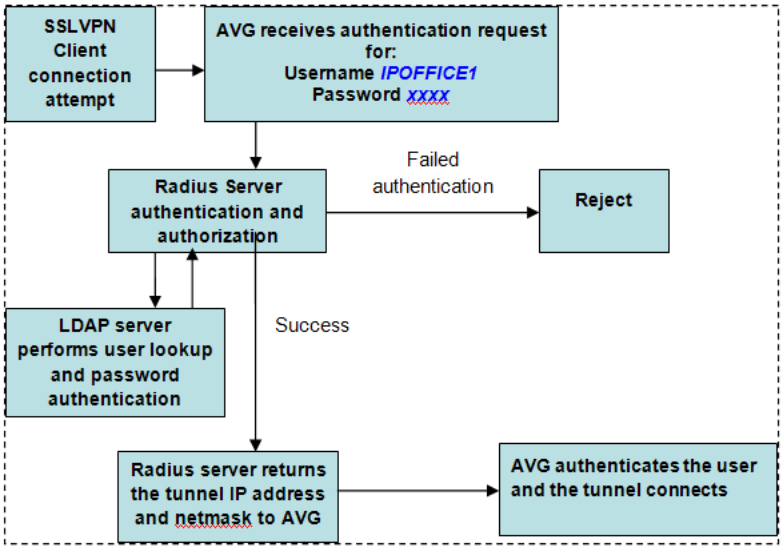
The key benefit of RADIUS authentication is that the SSL VPN service is always assigned the same tunnel IP address.

To configure RADIUS authentication, you must install a RADIUS server. Avaya recommends the Avaya Identity Engine for a Radius Server. For information and software download, go to http://support.avaya.com.

RADIUS protocol authentication information such as user account information as well as SSL VPN tunnel information such as IP address and netmask need to be stored in a database. There are two possible options:

- Use Identity Engine's local database to store the user information and provide both lookup and authentication and authorization services. This option can be used for a small number of users. Identity Engine has a hard limit of users. Consult the documentation for the exact value.
- Use an LDAP server to store user credentials and SSL VPN tunnel information for both lookup and authentication services. This option fits deployment scenarios for a large number of users.

For LDAP server installation, Avaya Identity Engine Radius Server documentation contains configuration options for LDAP servers from different vendors. RADIUS authentication using an LDAP server is illustrated in the figure below. Note that this RADIUS server configuration in this procedure does not require an LDAP server.



This procedure covers the manual steps to configure RADIUS authentication. Alternatively, you can configure authentication using the AVG authentication wizard.

This procedure is duplicated in Appendix C Configuring RADIUS authentication (with screens) on page 95. This version of the procedure includes screen captures of the user interface.

Procedure

1. Log on to the AVG BBI as administrator.

2. On the **IP Pool Configuration** page, add a new IP Address Pool for RADIUS authentication.
3. On the **IP Pool** page, set the **Default IP Pool** to the RADIUS authentication IP address pool you created in step 2.
4. Modify the VPN. On the **Authentication Servers** > **Add New Authentication Server** page, complete the fields for the RADIUS server.
5. Configure the RADIUS authentication server settings. Note that Vendor Id 1872 is associated to vendor Alteon and identifies AVG. Select the **Settings** tab and complete the following fields.
   - **Vendor ID: 1872**
   - **Vendor Type: 1**
   - **Timeout: 10**
   - **Vendor Id for VPN Id: 1872**
   - **Vendor Type for VPN Id: 3**
6. Configure RADIUS network attributes. Select the **Network Attributes** tab and complete the following fields.

Vendor ID Settings	Vendor Type Settings
Client IP Address: 1872	Client IP Address: 4
Client Netmask: 1872	Client Netmask: 5
Primary NBNS Server: 1872	Primary NBNS Server: 6
Secondary NBNS Server: 1872	Secondary NBNS Server: 7
Primary DNS Server: 1872	Primary DNS Server: 8

7. Configure filter attributes. Select the Filter Attributes tab and complete the following fields>.
   - **Radius filter attribute: disabled**
   - **Vendor Id for Filter Attribute: 9**
   - **Vendor Type for Filter Attribute: 1**
8. Specify the Radius server address. Select the **Servers** tab on the **RADIUS Servers** page.
9. Click **Add** and on the **Modify RADIUS Server** page, enter the RADIUS server IP address and shared secret.
10. Select the **Authentication Order** tab and specify the preferred order for authentication methods.

RADIUS server configuration attributes

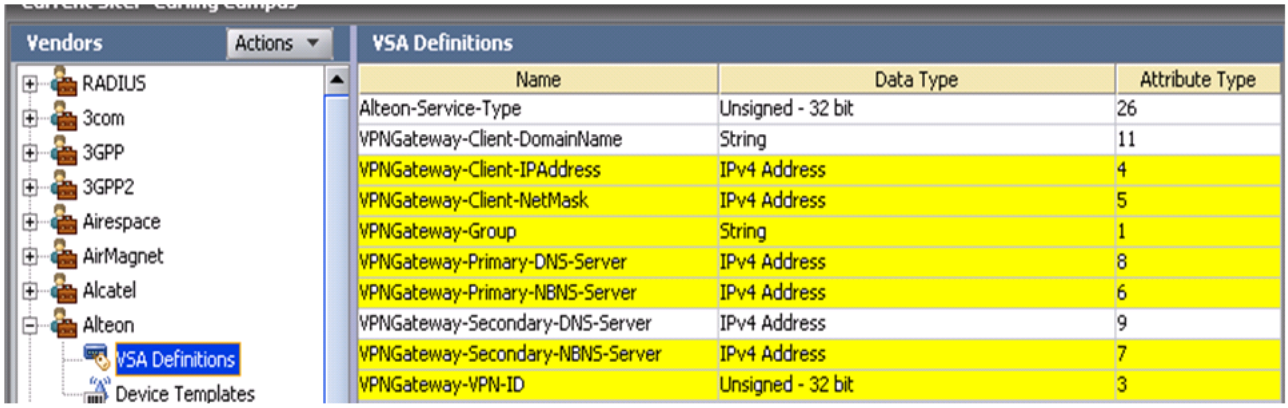
The SSL VPN service requires a RADIUS server. Avaya recommends that you use the Avaya Identity Engines Ignition Server as the RADIUS server.

When you connect the SSL VPN service, the Avaya VPN Gateway (AVG) authenticates the IP Office system by sending a query to an external RADIUS server. This section lists the attributes that you must configure on the RADIUS server.

RADIUS server attribute mapping

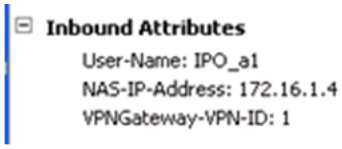
Vendor specific Radius attribute names and associated data types and vendor type codes for Alteon vendor (AVG) are contained in the list below.

The following examples have been obtained using an Avaya Identity Engines RADIUS server. The highlighted attributes have been configured as **Network Attributes** and **Settings** in the AVG RADIUS server configuration.



Name	Data Type	Attribute Type
Alteon-Service-Type	Unsigned - 32 bit	26
VPNGateway-Client-DomainName	String	11
VPNGateway-Client-IPAddress	IPv4 Address	4
VPNGateway-Client-NetMask	IPv4 Address	5
VPNGateway-Group	String	1
VPNGateway-Primary-DNS-Server	IPv4 Address	8
VPNGateway-Primary-NBNS-Server	IPv4 Address	6
VPNGateway-Secondary-DNS-Server	IPv4 Address	9
VPNGateway-Secondary-NBNS-Server	IPv4 Address	7
VPNGateway-VPN-ID	Unsigned - 32 bit	3

• Inbound Attributes coming from the AVG to the Radius Server during the authentication request are shown below.



The Radius attributes sent by AVG are:

- o NAS-IP-Address (generic radius attribute) is the AVG IP address.
- User-Name (generic radius attribute) is the user account name
- VPNGateway-VPN-ID is an Alteon attribute

The IDEngine Radius server has a default internal attribute mapping for the most popular Radius attributes as seen in the table below. The highlighted rows correspond to the Radius attributes contained in the Radius REQUEST above.

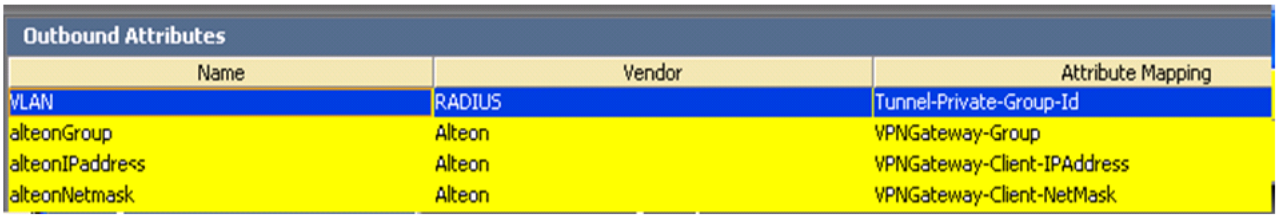
Inbound Attributes

Name	Vendor	Attribute Mapping
Inbound-Digest-Auth-Param	RADIUS	Digest-Auth-Param
Inbound-Digest-Domain	RADIUS	Digest-Domain
Inbound-Digest-Method	RADIUS	Digest-Method
Inbound-Digest-Nonce-Count	RADIUS	Digest-Nonce-Count
Inbound-Digest-Opaque	RADIUS	Digest-Opaque
Inbound-Digest-Qop	RADIUS	Digest-Qop
Inbound-Digest-Realm	RADIUS	Digest-Realm
Inbound-Digest-SIP-AOR	RADIUS	Digest-SIP-AOR
Inbound-Digest-URI	RADIUS	Digest-URI
Inbound-Digest-Username	RADIUS	Digest-Username
Inbound-Framed-Compression	RADIUS	Framed-Compression
Inbound-Framed-Interface-Id	RADIUS	Framed-Interface-Id
Inbound-Framed-IP-Address	RADIUS	Framed-IP-Address
Inbound-Framed-IP-Netmask	RADIUS	Framed-IP-Netmask
Inbound-Framed-MTU	RADIUS	Framed-MTU
Inbound-Framed-Pool	RADIUS	Framed-Pool
Inbound-Framed-Protocol	RADIUS	Framed-Protocol
Inbound-Login-IP-Host	RADIUS	Login-IP-Host
Inbound-NAS-Identifier	RADIUS	NAS-Identifier
Inbound-NAS-IP-Address	RADIUS	NAS-IP-Address
Inbound-NAS-Port	RADIUS	NAS-Port
Inbound-NAS-Port-Id	RADIUS	NAS-Port-Id
Inbound-NAS-Port-Type	RADIUS	NAS-Port-Type
Inbound-Port-Limit	RADIUS	Port-Limit
Inbound-Service-Type	RADIUS	Service-Type
Inbound-Tunnel-Client-Auth-Id	RADIUS	Tunnel-Client-Auth-Id
Inbound-Tunnel-Client-Endpoint	RADIUS	Tunnel-Client-Endpoint
Inbound-Tunnel-Medium-Type	RADIUS	Tunnel-Medium-Type
Inbound-Tunnel-Preference	RADIUS	Tunnel-Preference
Inbound-Tunnel-Private-Group-Id	RADIUS	Tunnel-Private-Group-Id
Inbound-Tunnel-Server-Auth-Id	RADIUS	Tunnel-Server-Auth-Id
Inbound-Tunnel-Server-Endpoint	RADIUS	Tunnel-Server-Endpoint
Inbound-Tunnel-Type	RADIUS	Tunnel-Type
Inbound-User-Name	RADIUS	User-Name

Radius servers evaluate the inbound attributes using authorization rules. The rule can use an inbound attribute to check a condition or can return the inbound attribute in a Radius RESPONSE as an outbound value. If an inbound attribute sent by AVG requires evaluation but is not part of the default Radius Server set it must be defined as a new inbound attribute on the Radius server. For examples of authentication rules, see *IDEngine Administration*.

• Outbound Attributes sent to the AVG from the Radius Server during an authentication RESPONSE are shown below:

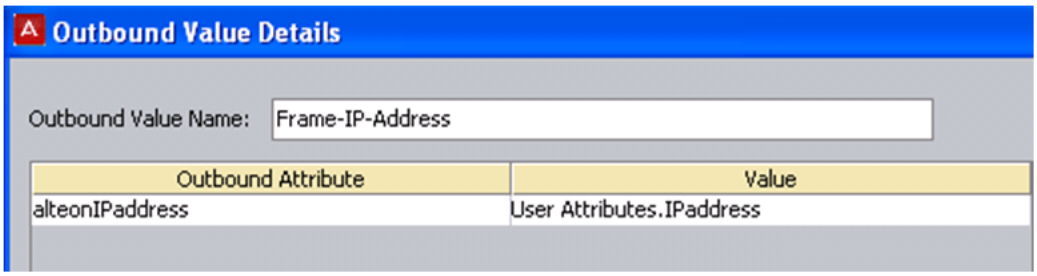
Outbound attributes are the data fields the radius server uses to carry provisioning data to the VPN Gateway. The outbound attributes are generic or vendor type radius protocol attributes. Similar with the inbound attributes the outbound attributes need to be created if they are not part of the default set of the Radius server. In the example above the three Alteon outbound attributes (specific for AVG): “alteonGroup”, “alteonIPaddress” and “alteonNetmask” need to be created in the Radius server as in the example below:



Outbound Attributes

Name	Vendor	Attribute Mapping
VLAN	RADIUS	Tunnel-Private-Group-Id
alteonGroup	Alteon	VPNGateway-Group
alteonIPaddress	Alteon	VPNGateway-Client-IPAddress
alteonNetmask	Alteon	VPNGateway-Client-NetMask

The outbound attribute values can be set to static values or can be mapped to user attributes in the local radius server database or in an LDAP repository. An example of an outbound attribute value mapped to a database user attribute is shown below:



Outbound Value Details

Outbound Value Name: Frame-IP-Address

Outbound Attribute	Value
alteonIPaddress	User Attributes.IPaddress

Outbound values are associated with authentication rules and are sent to the VPN Gateway as radius attributes when the rule is evaluated. If the rule evaluates to “Allow” the outbound values are used to set characteristics of the user’s session. When the rule is evaluated to “Deny” the returned outbound values are typically used to convey information on the cause of the denial. For more information, see the IDEngine documentation.

Chapter 5: Configuring an SSL VPN for Avaya support

This section provides information about the configuration process for IP Office when the service provider is Avaya. You can automatically configure the SSL VPN using the on-boarding process.

You can configure multiple instances of the SSL VPN service and run them concurrently.

Prerequisites

When you configure an SSL VPN service, the address of the VPN gateway can be an FQDN. You must configure the DNS server to resolve FQDN addresses. Configure the DSN settings in the IP Office Manager **System** form, under **DNS**.

Configuring an SSL VPN using an on-boarding file

The on-boarding XML file is available from Avaya. It contains the settings required to establish a secure tunnel between IP Office and an AVG server. When you import the on-boarding XML file, it applies the settings and installs a TLS certificate.

When you configure the SSL VPN service on a new system, you must begin by generating an inventory of the IP Office system. When you register your IP Office system, the inventory file that you generated is uploaded to the GRT and the inventory data is populated in the Avaya Customer Support (ACS) database. After you enable remote support, you can download the XML on-boarding file from the GRT web site and import it into your IP Office system.

The on-boarding process configures:

- VPN settings
- short codes for enabling and disabling the SSL VPN
- SNMP alarm traps

You can modify the automatically configured settings using IP Office Manager. To modify the settings, see the procedures in Configuring an SSL VPN for Avaya partner support on page 37.

Perform this procedure from the Avaya IP Office Web Manager interface.

Before you begin

Before you begin, you must have the hardware codes and catalog description of your IP Office system. For example, “IP OFFICE 500 VERSION 2 CONTROL UNIT TAA” is a hardware code and catalog description.

Procedure

1. Select **Tools > On-boarding**.
   The On-boarding dialog box displays.
2. If the hardware code for your IP Office system ends with the letters TAA, select the checkbox next to the prompt **Are you using TAA series hardware?**
3. Click **Get Inventory File** to generate an inventory of your IP Office system.
4. Click **Register IP Office**.
   A browser opens and navigates to the GRT web site.
5. Log in to the web site and enter the required data for the IP Office system.
6. Select **Remote Support** for the IP Office system.
7. Click **Download** and save the on-boarding file.
8. Browse to the location where you saved the on-boarding file and click **Upload**.
   A message displays to confirm that the on-boarding file has installed successfully.

Using the on-boarding file to modify an existing service

You can use the on-boarding file to configure the SSL VPN service. The on-boarding file contains the settings required to establish a secure tunnel between IP Office and an AVG server. Use this procedure when you have already configured the SSL VPN service on an IP Office system and need to update or modify the SSL VPN configuration.

Perform this procedure from the Avaya IP Office Web Manager interface.

Before you begin

Before you begin, you must have the hardware codes and catalog description of your IP Office system. For example, “IP OFFICE 500 VERSION 2 CONTROL UNIT TAA” is a hardware code and catalog description.

Procedure

1. Select **Tools > On-boarding**.
   The On-boarding dialog box displays.

2. This step is optional. To generate an inventory of your IP Office system, do the following:
    - If the hardware code for your IP Office system ends with the letters TAA, select the checkbox next to the prompt **Are you using TAA series hardware?**
    - Click **Get Inventory File**.
3. Click **Modify**.
   A browser opens and navigates to the Avaya web site.
4. Log in to the web site.
   The IP Office Remote Connectivity / Password Management page displays.
5. Click **Existing IP Office SSL VPN Remote Connectivity**.
6. Select **Regenerate on-boarding file (existing properties)**.
7. Enter the SSL VPN service name and the SSL VPN account name in the appropriate fields.
8. Click **Submit**.
9. Select whether you want to receive the updated on-boarding file by email, or whether you want to download the updated file and follow the prompts on the screen.
10. When you have either downloaded or received the updated on-boarding file, save it to your local system.
11. Browse to the location where you saved the on-boarding file and click **Upload** on the Web Manager interface.
    A message displays to confirm that the on-boarding file has installed successfully.

Chapter 6: Configuring an SSL VPN for Avaya partner support

This section provides information about the configuration process for IP Office when the service provider is not Avaya. For third party service provider support, the SSL VPN must be manually configured using Manager. The configuration process is the same in both Manager and IP Office Manager for Server Edition mode. Perform these procedures from the Manager interface. If you are configuring a Server Edition system, use IP Office Manager for Server Edition mode. Manual configuration is not supported for Basic Edition mode.

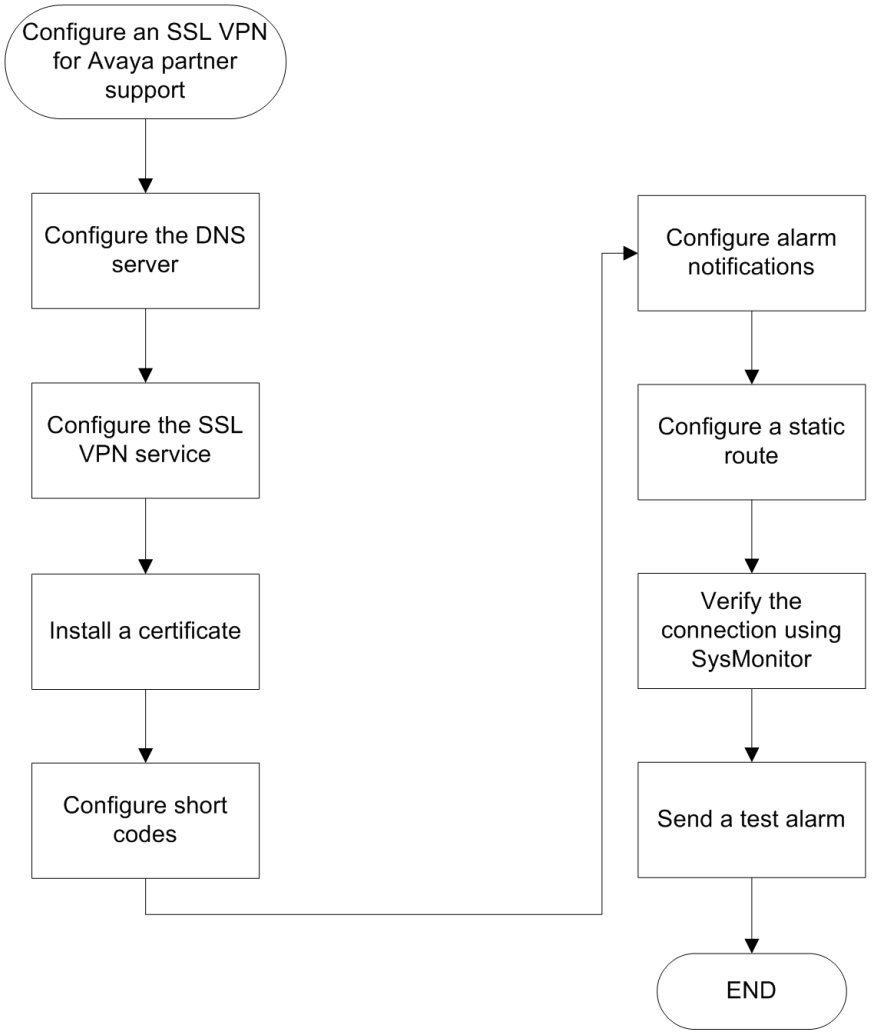
You can configure multiple instances of the SSL VPN service and run them concurrently.

Prerequisites

When you configure an SSL VPN service, the address of the VPN gateway can be an FQDN. You must configure the DNS server to resolve FQDN addresses. Configure the DSN settings in the IP Office Manager **System** form, under **DNS**.

Configuring an SSL VPN for Avaya partner support procedures

This task flow shows you the sequence of procedures you perform to configure an SSL VPN for partner support.



Navigation

- Configuring the DNS server
- Configuring the SSL VPN service on page 39
- Installing a certificate on page 41
- Configuring short codes on page 42
- Configuring alarm notifications on page 46
- Configuring a static route on page 50
- Verifying the connection using on page 53
- Sending a test alarm on page 54

Configuring the SSL VPN service

Use this procedure to configure the SSL VPN service.

Perform this procedure on the Manager interface. If you are configuring a Server Edition system, use IP Office Manager for Server Edition mode.

Before you begin

You must know the value of the following configuration variables.

Table 1: Service tab

Variable	Description
Service name	Enter a name for the new SSL VPN service.
Account name	Enter the SSL VPN service account name. This account name is used for authenticating the SSL VPN service when connecting with the AVG. **Server Edition systems:** If you are configuring a Server Edition system, Avaya recommends that you configure the same name for both the SSL VPN service account and the SNMP Agent Device ID. When these settings match, technical support personnel can use this information to identify the address of the SSL VPN tunnel. You can configure only one SNMP Agent Device ID per system. If you are configuring multiple instances of the SSL VPN service, choose one of the SSL VPN service account names to match to the SNMP Agent Device ID based on your needs for remote technical support. You can also view the Device ID by selecting **Network** from the navigation list and selecting a Server Edition system; the screen displays a summary of settings for the selected system.
Account password	Enter the password for the SSL VPN service account.
Confirm password	Confirm the password for the SSL VPN service account.
Server address	Enter the address of the VPN gateway. The address can be an FQDN or an IPv4 address.
Server type	Select AVG.
Server port number	Select a port number. The default port number is 443.

Table 2: Session tab

Variable	Description
Preferred Data Transport Protocol	Select TCP; this is the protocol used by the SSL VPN service for data transport. If you select UDP as the protocol when you configure the connection, UDP displays in this field but the SSL VPN service falls back to TCP.
Heartbeat Interval	Enter the length of the interval between heartbeat messages in seconds. The default value is 30 seconds.
Heartbeat Retries	Enter the number of unacknowledged heartbeat messages that IP Office sends to AVG before determining that AVG is not responsive. When this number of consecutive heartbeat messages is reached and AVG has not acknowledged them, IP Office ends the connection. The default is 4.
Reconnect Interval on Failure	The interval to wait before the SSL VPN service attempts to re-establish a connection with the AVG. The interval begins when the SSL VPN tunnel is in-service and makes an unsuccessful attempt to connect with the AVG, or when the connection with the AVG is lost. The default is 60 seconds.

Procedure

1. In the navigation list, right-click **Service**.
2. Select **New** > **SSL VPN Service**.
3. On the **Service** tab, configure the settings listed in the table below.
4. Select the **Session** tab and configure the settings listed in the table below.
5. Select the **Fallback** tab and choose one of the following options:
   - to enable the service and establish an SSL VPN connection, ensure that the **In Fallback** option is de-selected
   - to configure the service without establishing an SSL VPN connection, select the **In Fallback** option
6. Click **OK**.
7. Click the **Save** icon to save the configuration.

Installing a certificate

The SSL VPN service uses digital certificates to verify the identity of the devices at each end of the SSL VPN tunnel. This procedure describes how to install a certificate in the IP Office trusted certificate store.

Manager and IP Office Manager for Server Edition contain a menu option that allows you to restore the default security settings in IP Office. If you restore security settings to their defaults, the certificate is removed from the trusted certificate store and the SSL VPN service disconnects immediately. You cannot reconnect the SSL VPN service until you install the required certificate in the trusted certificate store.

Similarly, the Security Manager application allows you to delete the certificate from the trusted certificate store. If you delete the certificate using Security Manager, the SSL VPN service disconnects the next time that the tunnel renegotiates the secret key. This renegotiation occurs every 8 hours by default, and may occur at a different interval depending on the settings configured in the AVG. When the SSL VPN service disconnects during a renegotiation, or if you disable the service before the next renegotiation occurs, you cannot enable the SSL VPN service again until you have installed the required certificate in the trusted certificate store.

Before you begin

You must install one of the following types of certificate:

- a self-signed AVG certificate
- the certificate of the CA that signed the AVG certificate

Procedure

1. Select **File > Advanced > Security Settings**.
   A dialog box lists the IP Office systems.
2. Click the checkbox to select the IP Office system where you want to install the certificate.
3. Click **OK**.
   A dialog box displays.
4. In the **Service User Name** field, enter the user name of the IP Office administrator.
5. In the **Service User Password** field, enter the password of the IP Office administrator.
6. Click **OK**.
   The credentials are accepted.
7. In the navigation panel, select **Security > System** and select the configuration name.

8. On the **Certificates** tab, click **Add**.
   A dialog box displays, prompting you to select a source for the certificate.
9. Select **Paste from clipboard** and click **OK**.
   A dialog box opens to capture the text of the certificate.
10. Copy your certificate and paste the text into the open window. You must include the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.
11. Click **OK**.
    The certificate name displays in the Installed Certificates list.

Configuring short codes

The IP Office system allows you to configure short codes. These short codes trigger a specific action when you dial the short code on a deskphone that is connected to the IP Office system. For information on programming phone buttons with short codes, see the IP Office Manager documentation.

You can configure short codes and use them to enable and disable the SSL VPN service. When you use the short codes to enable or disable the SSL VPN service, the service remains provisioned in the system; the short codes put the tunnel in-service or in a fallback state.

The IP Office system includes a set of pre-defined features that you can access through short codes. You can use the following pre-defined features to create short codes that enable and disable the SSL VPN service:

- Clear HuntGroup Night Service: enables the SSL VPN service
- Set HuntGroup Night Service: disables the SSL VPN service

These short codes are available for internal use and you must dial them from a desk phone that is connected to the IP Office system. If you want to use the short codes from an external phone, you can configure an auto-attendant. The auto attendant allows you to dial into the IP Office system from an external phone number and activate the short codes using a menu system.

Related topics:

Configuring a short code to enable the SSL VPN service on page 43
Configuring a short code to disable the SSL VPN service on page 43
Configuring an auto attendant on page 44

Configuring a short code to enable the SSL VPN service

Use this procedure to configure a short code that enables the SSL VPN service when the code is dialed from a deskphone connected to the IP Office system.

Procedure

1. In the navigation list, select **Short Code**.
   The list of default short codes displays.
2. Right-click and select **New**.
   The Short Code tab displays.
3. In the **Code** field, enter ***775x1**, where *x* represents an instance of the SSL VPN service, ranging from 1 to 9. For example, if you have two instances of the SSL VPN service configured, and are configuring short codes for the first instance, enter ***77511**.

   Note:

   You can assign different numbers to the shortcode. For ease of use, Avaya recommends that you use *775, which represents *SSL on a dialpad.
4. In the **Feature** list, select **Clear HuntGroup Night Service**.
5. In the **Telephone Number** field, enter the name of the SSL VPN service in quotation marks. For example, if the service name is Service1, enter `"Service1"`.

   Use the name of the SSL VPN service that you entered when you created the SSL VPN service. See Configuring the SSL VPN service on page 39 for information about this setting.
6. Click **OK**.
7. Click the **Save** icon to save the configuration changes.

Configuring a short code to disable the SSL VPN service

Use this procedure to configure a short code that disables the SSL VPN service when the code is dialed from a deskphone connected to the IP Office system.

Procedure

1. In the navigation list, select **Short Code**.
   The list of default short codes displays.
2. Right-click and select **New**.

The Short Code tab displays.

3. In the **Code** field, enter ***775x0**, where *x* represents an instance of the SSL VPN service, ranging from 1 to 9. For example, if you have two instances of the SSL VPN service configured, and are configuring short codes for the first instance, enter ***77510**.

   Note:

   You can assign different numbers to the shortcode. For ease of use, Avaya recommends that you use *775, which represents *SSL on a dialpad.

4. In the **Feature** list, select **Set HuntGroup Night Service**.
5. In the **Telephone Number** field, enter the name of the SSL VPN service in quotation marks. For example, if the service name is Service1, enter `"Service1"`.

   Use the name of the SSL VPN service that you entered when you created the SSL VPN service. See Configuring the SSL VPN service on page 39 for information about this setting.
6. Click **OK**.
7. Click the **Save** icon to save the configuration changes.

Configuring an auto attendant

Use this procedure to configure an auto attendant. The auto attendant allows you to access into the IP Office system from an internal or external phone number and use a menu system to enable or disable the SSL VPN service.

Before you begin

You must configure short codes. See Configuring short codes on page 42.

If you are using Avaya Voicemail Pro, you must configure a module for assisted transfer before you begin this procedure. For more information, see *Voicemail Pro Administration* (15–601063).

About this task

In this procedure, you create an auto attendant, and then map incoming calls to the auto attendant. This example uses 0 to enable the SSL VPN service and 1 to disable it, but you can assign these functions to any key on the dialpad.

Procedure

1. Select one of the following options:
   - If you use Embedded Voicemail, select **Auto Attendant** in the navigation list.

- If you use Voicemail Pro, begin this procedure at step 12 on page 45.

2. Right-click and select **New**.
3. In the **Name** field, enter the name for the auto attendant.
4. Select the **Actions** tab.
5. Select the entry for the **0** key and click the **Edit** button.
6. From the **Action** list, select one of the following options:
   - Select **Normal Transfer** transfer.
   - Select **Transfer**.
7. In the **Destination** list, type the short code that you configured to enable the service and click **OK**.
8. Select the entry for the **1** key and click the **Edit** button.
9. From the **Action** list, select one of the following options:
   - Select **Normal Transfer** transfer.
   - Select **Transfer**.
10. In the **Destination** list, type the short code that you configured to disable the service and click **OK**.
11. Click the **Save** icon to save the configuration changes.
12. In the navigation list, select **Incoming Call Route**.
13. On the **Standard** tab, set the **Bearer Capability** field to **Any Voice**.
14. In the **Line Group ID** list, select the line that you want to use for enabling and disabling the SSL VPN service.
15. Select the **Destination** tab.
16. Choose one of the following options:
    - If you use Embedded Voicemail, select the auto attendant that you configured from the **Destination** list.
    - If you use Voicemail Pro, type `VM:<name>` in the **Destination** list, where `<name>` is the name of the Voicemail Pro module.
17. Click **OK**.
18. Click the **Save** icon to save the configuration changes.

Next steps

You can record prompts for the auto attendant. For more information about recording prompts, see the documentation for your voicemail system. If you are using Embedded Voicemail, see the *Embedded VoicemailInstallation Guide*. If you are using Voicemail Pro, see *Voicemail Pro Administration*.

Configuring alarm notifications

It is optional to configure fault management for the SSL VPN service. If you do configure fault management, you can set filters to determine the types of events that you are notified about. For example, you can receive notifications about faults related to the SSL VPN service, or you can receive notifications about faults related to the IP Office system.

When you configure fault management, you must define alarm destinations where system faults are reported. You can configure the following destinations for alarm reporting:

- SNMP traps reported on a local LAN, or on a remote server
- email notifications reported to an SMTP server on a local LAN, or a remote SMTP server
- syslog entries reported on a local LAN, or on a remote server

The alarm destinations that you can configure depend on the operating mode that you use. The following table lists the alarm destinations supported in each mode.

Alarm destination	Operating mode			
	Essential Edition	IP Office Server Edition	Server Edition Expansion System	Basic Edition
SNMP traps				
SNMP on a local LAN	✔	✔	✔	✔
SNMP over an SSL VPN service	✔	✔	✔	✔
Email notifications				
SMTP server on a local LAN	✔	✔	✔	—
SMTP server over an SSL VPN tunnel	✔	✔	✔	—
Syslog entries				
Syslog server on a local LAN	✔	✔	✔	—
Syslog server over an SSL VPN tunnel	✔	✔	✔	—

Related topics:

Configuring SNMP trap destinations on page 47
Configuring email alarm notifications on page 48
Configuring syslog entries on page 49

Configuring SNMP trap destinations

Use the following procedure to report system faults as SNMP traps. You can set filters to determine the types of events that generate SNMP traps. For example, you can generate SNMP traps for faults related to the SSL VPN service, or you can generate SNMP traps for faults related to theIP Office system.

Before you begin

When you define a destination IP address for a fault event, the system uses an IP routing table to determine which interface to use when sending the fault event. The destination must be an IPv4 address for the SNMP trap to be correctly routed to the fault management server.

You must configure a trap listener on the destination computer where the SNMP traps are reported.

Procedure

1. In the navigation list, click **System** and select the **System Events** tab. Manager displays a **Configuration** tab and an **Alarms** tab.
2. On the **Configuration** tab, select the **SNMP Enabled** option.
3. In the **Community** field, enter `public`.
4. On the **Alarms** tab, click **Add**.
5. Select **Trap** and enter a destination address for the SNMP traps in the **IP Address** field. .
6. Enter a port number or use the default port number (162).
7. In the **Community** field, enter `public`.
8. In the **Events** list, choose the event filter:
   - Select **Service** to generate SNMP traps for faults related to the SSL VPN service.
   - Select any events related to the operation of the IP Office system for which you want to generate SNMP traps. For information about these options, see *IP Office Manager*.
9. Click **OK** to close the dialog box.
10. Click **OK** on the Alarms tab.

11. click the **Save** icon to save the configuration changes.

Configuring email alarm notifications

Use the following procedure to receive email notifications about faults when they occur. You can set filters to determine the types of events that you are notified about. For example, you can receive notifications about faults related to the SSL VPN service, or you can receive notifications about faults related to the IP Office system.

Before you begin

You must configure an SMTP email server on the computer that you are using for fault management. You must also configure an email client on the computer where you want to receive the email notifications.

When you define a destination address for a fault event, the system uses an IP routing table to determine which interface to use when sending the fault event. The destination must be an IPv4 address for the notification to be correctly routed to the fault management server.

Procedure

1. In the navigation list, click **System** and select the **System Events** tab. Manager displays a **Configuration** tab and an **Alarms** tab.
2. On the **Alarms** tab, click **Add**.
3. Select the **Email** option and enter the address where you want to receive email notifications in the **Email** field.
4. In the **Events** list, choose the event filter:
   - Select **Service** to receive notifications about faults related to the SSL VPN service.
   - Select any events related to the operation of the IP Office system that you want to receive notifications about. For information about these options, see *IP Office Manager*.
5. Click **OK** to close the dialog box.
6. Click **OK** on the Alarms tab.
7. Select the **SMTP** tab.
8. In the **IP Address** field, enter the IP address of the SMTP server.
9. In the **Port** field, enter the port number of the SMTP server.
10. In the **From Address** field, enter the email address that the IP Office system will use to send email notifications.
11. Select **Server Requires Authentication**.

12. In the **User name** and **Password** fields, enter the credentials required to log in to the SMTP server.
13. Click **OK**.
14. Click the **Save** icon to save the configuration changes.

Configuring syslog entries

Use the following procedure to report system faults as syslog entries. You can set filters to determine the types of events that are reported. For example, you can report faults related to the SSL VPN service, or you can report faults related to the IP Office system.

Before you begin

You must configure a syslog client on the server where you want the system faults to be reported.

When you define a destination IP address for a fault event, the system uses an IP routing table to determine which interface to use when sending the fault event. The destination must be an IPv4 address for the notification to be correctly routed to the fault management server.

Procedure

1. In the navigation list, click **System** and select the **System Events** tab. Manager displays a **Configuration** tab and an **Alarms** tab.
2. On the **Alarms** tab, click **Add**.
3. Select the **Syslog** option and enter the IP address of the server where the syslog client is configured in the **IP Address** field.
4. Enter the port number of the server where the syslog client is configured in the **Port** field.
5. In the **Events** list, choose the event filter:
   - Select **Service** to report faults related to the SSL VPN service.
   - Select any events related to the operation of the IP Office system that you want to receive notifications about. For information about these options, see *IP Office Manager*.
6. Click **OK** to close the dialog box.
7. Click **OK** on the **Alarms** tab.
8. Click the **Save** icon to save the configuration changes.

Configuring a static route

When you configure split tunneling routes on the AVG, the IP Office system learns the routing information for the tunnel dynamically when the SSL VPN service connects with the AVG. However, you also have the option to configure a static route. This section provides information to help you determine whether to configure a static route, and provides a procedure for configuring one.

When you configure a static route, the system uses the IP route information configured in Manager to determine the destination for forwarded traffic. You can define the SSL VPN service as the destination.

Use a static route when:

- split tunneling routes are not advertised by the AVG and you need to send traffic through the tunnel
- the SSL VPN service is not connected to the AVG and you want to queue traffic to be forwarded through the tunnel when the connection is restored

Before you begin

Before you begin, you must have the following information:

- the address of the remote subnet; this is the subnet located in the private network where the AVG is installed
- the subnet mask applied to the subnet address
- the SSL VPN service name that you want to use to send traffic to this remote subnet

Procedure

1. In the navigation list, select **IP Route**.
2. Right-click and select **New**.
3. In the **IP Address** field, enter the address of the remote subnet located on the site where the AVG is installed.
4. In the **Subnet mask** field, enter the subnet mask applied to the remote subnet.
5. In the **Gateway IP Address** field, ensure that the gateway IP address is set to 0.0.0.0.
6. From the **Destination** list, select the name of the SSL VPN service.

Chapter 7: Network address and port translation (NAPT) rules

Use an SSL VPN service and network address and port translation (NAPT) rules to establish remote communication sessions with LAN devices such as an IP Office UCM module. To connect to a LAN device on the private IP Office network, the support service provider launches a communication application on a PC located at the remote service provider site and specifies the following configuration parameters for the session:

- the IP address of an SSL VPN tunnel
- the external port number for the LAN device

IP Office uses the NAPT rules to map the tunnel IP address and the external port number to the correct IP address and port number on the private network.

Configuring NAPT rules

Perform this procedure on the Manager interface.

When you configure an NAPT rule, you must select an application type. The following application options are available:

- Custom
- VMPro
- One-X Portal
- SSH
- TELNET
- RDP (Remote Desktop Protocol)
- Web Control

You can use the **Custom** setting to configure a NAPT rule for a new application type. You can also use the **Custom** setting with a modified **External Port Number** to open two concurrent communication sessions using the same application to connect to the same LAN device. For example, to enable two concurrent SSH sessions to the same IP address, the two NAPT rules would look similar to the following.

Application	Protocol	External Port Number	Internal IP address	Internal Port Number
SSH	TCP	22	192.168.40.1	22
Custom	TCP	221	192.168.40.1	22

Procedure

1. In the navigation list, select **Service**.
2. In the **Service** list, select the SSL VPN service where you want to configure NAPT rules.
3. In the details pane for the service, select the **NAPT** tab.
4. Under **Application**, open the drop down list and select an application type.

   The **Protocol** field and the **Port Number** fields are automatically filled with the default values.
5. (Optional) If you want to configure a **Custom** application, modify the **External Port Number** field.
6. Repeat steps 4 and 5 to configure additional rules.

Deleting an NAPT rule

Procedure

To delete an NAPT rule, use the empty column on the left side of the table. Right click in the empty cell next to the rule you want to delete and select the delete icon.

Chapter 8: Verify the connection between IP Office and AVG

Use the procedures in this chapter to test the connection between the IP Office system and AVG.

Verifying the connection using SysMonitor

You can use the System Status Application (SSA) to verify that the SSL VPN tunnel is in service. Launch the SSA and verify that the Tunnel configuration settings are listed.

You can also perform the steps below to use SysMonitor to verify the SSL VPN connection between the IP Office system and the AVG.

Procedure

1. Select **Start > Programs > IP Office > Monitor**.
   The SysMonitor application connects to the IP Office server and displays a system log.
2. Select **Filters > Trace** options and click the **VPN** tab.
3. In the SSL VPN area, verify that **Session** and **Session State** are enabled. Click **OK**.
   The SysMonitor log lists the activity for the SSL VPN service under the name that you configured for the service.
4. Locate the service name and check the following information:

Session state change	When you enable the SSL VPN service, the session state progresses through the following stages: • resolving the domain name • starting the session • connecting the IP address of IP Office to the VPN gateway IP address If IP Office cannot resolve the domain name, the following error message displays: “DNS failed to resolve host

	name <x.x.x> and reached MAX retries. Restart session.”

Verifying the AVG SSL VPN deployment using System Status Application

Perform the following actions to test the AVG SSL deployment.

1. Launch the IP Office System Status Application (SSA) and verify that the SSL VPN tunnel is **In Service** and the **Tunnel IP Address** is displayed.
2. Ping the IP Office remotely. From the Service Agent computer, launch a command window and execute a ping command using the tunnel IP address. The ping should be successful.

Verifying the connection using the AVG BBI

Procedure

1. Log in to the AVG BBI.
2. In the navigation pane on the left, expand **Monitor**.
3. Under **Monitor**, select **Users**.
4. The **Source IP** column displays:
   - the IP Office IP address
   - the SSL VPN tunnel IP address assigned to the local user.

Sending a test alarm

Use this procedure to send a test alarm from the System Status Application (SSA). Use the test alarm to generate a fault event.

Before you begin

You must have an alarm destination defined. When you define a destination IP address for the fault event, the system uses an IP routing table to determine which interface to use when sending the fault event.

Procedure

1. Launch SSA using one of the following methods:
   - Launch SSA from the IP Office Admin DVD.
   - Select **Start > Programs > IP Office > System Status**.
   - From within Manager or IP Office Manager for Server Edition, select **File > Advanced > System Status**.
2. Select **Alarms > Service** from the navigation list.
3. Click the **Test Alarm** button.

   The table displays the results of the test:

Value	Description
Last Date of Error	The date and time that the alarm occurred.
Occurrences	The number of times that the alarm has occurred since the control unit was last restarted or the alarm was last cleared.
Error Description	Test alarms display the message “Operator initiated test alarm.”

   If you configured an alarm destination for an SNMP trap, the test alarm generates the following information:

```
Enterprise: ipoGenTraps
Bindings (8)
Binding #1: ipoGTEventStdSeverity.0 *** (int32) major(4)
Binding #2: ipoGTEventDateTime.0 *** (octets)
Binding #3: ipoGTEventDevID.0 *** (octets)
Binding #4: sysDescr.0 *** (octets)
Binding #5: ipoGTEventReason.0 *** (int32) testAlarm(39)
Binding #6: ipoGTEventData.0 *** (octets)
Binding #7: ipoGTEventAlarmDescription.0 *** (octets) Operator initiated
test alarm - do not process
Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) (zero-length)
```

Chapter 9: Monitoring and managing the IP Office system

When the SSL VPN service is connected, you can monitor the IP Office system remotely through the tunnel. You can also manage and upgrade the IP Office system remotely. The SSL VPN service allows you to use thick applications and web-based applications as if they were directly connected to a local LAN interface. This section provides information about the supported applications and how to use them.

Monitoring tools

You can use the following tools to monitor the IP Office system remotely:

- System Status Application (SSA): The System Status Application is a diagnostic tool that you can use to monitor the status of IP Office systems. SSA reports real-time and historical events as well as status and configuration data.
- SysMonitor: The SysMonitor application displays operating information about the IP Office system. It can capture the information to log files for analysis.

Management tools

You can use the following tools to manage, upgrade, and configure the IP Office system remotely:

- IP Office Manager: An administrative application that allows you to configure system settings for IP Office Essential Edition systems.
  - IP Office Manager for Server Edition: When you launch IP Office Manager, you can choose to open a configuration using IP Office Manager for Server Edition mode. This mode allows you to administer Server Edition servers and expansion systems.
- IP Office Basic Edition – Web Manager: a browser-based tool that allows you to configure system settings for IP Office.

Fault reporting

You can use the SSL VPN service to send system faults to a remote fault management server located at the service provider site where the AVG is installed. You can set event filters to determine which faults are reported, and configure the destinations where faults are sent.

For information about fault reporting, see Configuring alarm notifications on page 46

Operating modes

The tools that you can use to monitor and manage the IP Office system remotely depend on the operating mode that you use. The following table lists the tools that are supported in each mode.

Tools	Operating mode			
	Essential Edition	IP Office Server Edition	Server Edition Expansion System	Basic Edition
SSA	✔	✔	✔	✔
SysMonitor	✔	✔	✔	✔
Manager (Simplified)	—	—	—	✔
Manager (Standard) and IP Office Manager for Server Edition	✔	✔	✔	—
Web Manager	—	—	—	✔
Fault reporting	✔	✔	✔	✔

Monitoring IP Office remotely using SSA

Use this procedure to connect the System Status Application (SSA) to IP Office through the SSL VPN tunnel.

Before you begin

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel
- the user name for the IP Office administrator account
- the password for the IP Office administrator account

Procedure

1. Launch SSA using one of the following methods:
   - Launch SSA from the IP Office Admin DVD.
   - Select **Start > Programs > IP Office > System Status**.
   - From within Manager or IP Office Manager for Server Edition, select **File > Advanced > System Status**.

2. In the **Control Unit IP Address** field, enter the IP address of the SSL VPN tunnel.
3. In the **User Name** field, enter the user name for the IP Office administrator account.
4. In the **Password** field, enter the password for the IP Office administrator account
5. Click **Logon**.

Monitoring IP Office remotely using SysMonitor

Use this procedure to connect the SysMonitor application to IP Office through the SSL VPN tunnel.

Before you begin

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel
- the password for the IP Office administrator account

Procedure

1. Select **Start > Programs > IP Office > Monitor**.
2. Click the **Select Unit** icon.
   A dialog box displays.
3. In the **Control Unit IP Address** field, enter the IP address of the SSL VPN tunnel.
4. In the **Password** field, enter the password for the IP Office administrator account.
5. Click the browse button next to the **Trace Log Settings Filename** field and browse to the location where you want to save the trace log and click **Open**.
6. Click **OK**.

Remotely monitoring LAN devices using the SSL VPN tunnel

Use this procedure to connect to a LAN device on the IP Office network through the SSL VPN tunnel using network address and port translation (NAPT). You can connect to a LAN device

using a communication application that has an NAPT rule configured for it. For information on configuring NAPT rules, see Network address and port translation (NAPT) rules on page 51.

Before you begin

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel
- the external port number configured in the NAPT rule for the LAN device you are connecting to

Procedure

1. Open the communication application you are using to connect to a LAN device through the SSL VPN tunnel.
2. Establish a communication session using the IP address of the SSL VPN tunnel and the external port number for the LAN device.

Configuring IP Office remotely using Web Manager

Use this procedure to connect the Web Manager application to IP Office through the SSL VPN tunnel.

For information about how to use the Web Manager application to configure the IP Office system, see *Avaya IP Office Basic Edition – Web Manager.*

Before you begin

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel
- the account name for the IP Office administrator account
- the password for the IP Office administrator account

Procedure

1. In a browser, enter the IP address for web management using the following format: `https://10.0.0.1:8443/webmanagement/WebManagement.html`, where *10.0.0.1* is the IP address of the SSL VPN tunnel.

   If the browser responds with a security warning, follow the menu settings displayed to continue with the connection.
2. When the login menu displays, enter the user name and password for system administration.
3. Click **Login**.

The home page for the system web management displays.

Configuring IP Office remotely using Manager

You can use Manager to administer the IP Office system remotely through the SSL VPN tunnel. When you use Manager through the SSL VPN tunnel, automatic discovery of IP Office systems is not supported. You must configure the IP address of the system that you want to connect to. Use this procedure to connect the Manager application to IP Office through the SSL VPN tunnel.

For information about how to configure Manager, and how to use it to administer an IP Office system, see *Avaya IP Office Manager*.

Before you begin

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel
- the account name for the IP Office administrator account
- the password for the IP Office administrator account

Procedure

1. Select **Start > Programs > IP Office > Manager**.
2. Click the icon to **Open Configuration from IP Office**.
   The Select IP Office dialog box displays.
3. Enter the IP address of the SSL VPN tunnel in the **Unit/Broadcast Address** field and click **Refresh**.
4. Select the IP Office system that you want to configure and click **OK**.
   The Configuration Service User Login dialog box displays.
5. Enter the user name for the IP Office administrator account in the **Service User Name** field, and enter the password for the IP Office administrator account in the **Service User Password** field. Click **OK**.

Configuring Server Edition systems remotely using IP Office Manager for Server Edition

You can use the IP Office Manager for Server Edition to administer the following systems remotely through the SSL VPN tunnel:

- Server Edition Primarys
- Server Edition Secondarys
- Server Edition Expansion Systems

Before you begin

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel
- the account name for the IP Office Manager for Server Edition administrator account
- the password for the IP Office Manager for Server Edition administrator account

About this task

To configure Server Edition systems remotely, you must configure an SSL VPN service between the AVG and the Server Edition Primary. You can then apply configuration changes to the Server Edition systems that are connected to the Primary Server. You must first configure an SSL VPN service between each Server Edition system and the AVG.

Use this procedure to connect the IP Office Manager for Server Edition to a Server Edition Primary through the SSL VPN tunnel.

For information about how to use IP Office Manager for Server Edition, see *Avaya IP Office Manager*.

Procedure

1. Select **Start > Programs > IP Office > Manager**.
2. Select **File > Preferences**.
3. Select **Use Remote Access for Multi-site** and click **OK**.
4. Click the icon to **Open Configuration from IP Office**.
   The Select IP Office dialog box displays.
5. Enter the IP address of the SSL VPN tunnel in the **Unit/Broadcast Address** field and click **Refresh**.
6. Select the Server Edition system that you want to configure.
   When you select the Server Edition system, the Open with Server Edition option displays and is enabled by default.
7. If you are connecting to a Server Edition Primary and want to make configuration changes to Server Edition systems that are connected to it, select **Use Remote**

Access. If you are connecting directly to the Server Edition system that you want to configure, you do not need to select this option.

8. Click **OK**.
   The Configuration Service User Login dialog box displays.
9. Enter the user name for the IP Office Manager for Server Edition administrator account in the **Service User Name** field, and enter the password for theIP Office Manager for Server Edition administrator account in the **Service User Password** field. Click **OK**.
10. In the navigation list, select **Network**.
    The Summary screen displays. A table at the bottom of the screen lists all Server Edition systems.
11. Select the Server Edition system that you want to configure.
    The Summary screen displays configuration information for the selected system.

Configuring Server Edition systems remotely using Web Control

You can use the Web Control interface to launch the IP Office Manager for Server Edition and administer Server Edition systems remotely through the SSL VPN tunnel.

You can use the IP Office Manager for Server Edition to administer the following systems remotely through the SSL VPN tunnel:

- Server Edition Primarys
- Server Edition Secondarys
- Server Edition Expansion Systems

Before you begin

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel
- the account name for the Web Control administrator account
- the password for the Web Control administrator account

About this task

To configure Server Edition systems remotely, you must configure an SSL VPN service between the AVG and the Server Edition Primary. You can then apply configuration changes to the Server Edition systems that are connected to the Primary Server. You must first configure an SSL VPN service between each Server Edition system and the AVG.

Use this procedure to launch the IP Office Manager for Server Edition through the Web Control interface and use it connect to a Server Edition Primary through the SSL VPN tunnel.

For information about how to use IP Office Manager for Server Edition, see *Avaya IP Office Manager*.

Procedure

1. Open a browser and enter `https://<IP address>:7070`, where <*IP address*> is the address of the SSL VPN tunnel configured for the Server Edition Primary.
2. Enter the administrator credentials in the **Logon** and **Password** fields and click **Login**.
   The Home screen displays and lists the Server Edition Servers and Expansion Systems.
3. Click **Manage**.
   The IP Office Manager for Server Edition opens and displays a Summary screen.
4. Select **File > Close** to close the configuration.
5. Select **File > Preferences**.
6. Select **Use Remote Access for Multi-site** and click **OK**.
7. Click the icon to **Open Configuration from IP Office**.
   The Select IP Office dialog box displays.
8. Enter the IP address of the SSL VPN tunnel in the **Unit/Broadcast Address** field and click **Refresh**.
9. Select the Server Edition server.
   When you select the Server Edition system, the Open with Server Edition option displays and is enabled by default.
10. Select **Use Remote Access** and click **OK**.
    The Configuration Service User Login dialog box displays.
11. Enter the user name for the IP Office Manager for Server Edition administrator account in the **Service User Name** field, and enter the password for the IP Office Manager for Server Edition administrator account in the **Service User Password** field. Click **OK**.
    The IP Office Manager for Server Edition opens and displays a Summary screen.
12. In the table at the bottom of the screen, select the Server Edition Primary.
13. From the **Open . . .** list on the right side of the screen, click **Configuration**.
    A navigation tree displays for the system.
14. After you have configured the selected system and saved your changes, select **Network** from the navigation list to return to the **Summary** screen.

15. To configure other Server Edition systems that are connected to the Server Edition Primary server, select the system from the table at the bottom of the Summary screen.
    The Summary screen displays configuration information for the selected system.

Chapter 9: Upgrading IP Office remotely

You use the SSL VPN tunnel to upgrade the IP Office system from the service provider site. This feature is available when you upgrade a Release 8.1 system to a higher software version.

When you use Manager through the SSL VPN tunnel, automatic discovery of IP Office systems is not supported.

Perform this procedure at the service provider site, using the Manager interface installed on the service agent server. If you are configuring a Server Edition system, use IP Office Manager for Server Edition mode.

Before you begin

At the service provider site, the IP Office Admin DVD containing the new software version must be installed on the Service Agent PC.

The SSL VPN tunnel must be in service, and you must have the following information:

- the IP address of the SSL VPN tunnel

Procedure

1. Select **File > Preferences > Discovery**.
2. In the **IP Search Criteria** field, enter the IP address of the SSL VPN tunnel and click **OK**.
3. Select **File > Advanced > Upgrade**.
   The Upgrade Wizard displays.

   Note:

   If a dialog box displays and prompts you to open a configuration file, click Cancel and proceed with this step. You do not need to open a configuration file before you perform an upgrade.
4. In the **Unit/Broadcast Address** field, enter the IP address of the SSL VPN tunnel and click **Refresh**.

   Do not enter a broadcast address. Broadcast addresses are not supported for remote upgrades over an SSL VPN connection.
5. Click a checkbox to select the system that you want to upgrade and click **Upgrade**.
   After the upgrade completes, IP Office reboots and the SSL VPN service automatically reconnects.

Chapter 10: Monitoring the SSL VPN service

In addition to monitoring the IP Office system, you can also monitor the SSL VPN tunnel. This section provides information about the monitoring tools available for the SSL VPN service and how to use them.

You can use the following tools to monitor the SSL VPN service:

- System Status Application (SSA): The System Status Application is a diagnostic tool that you can use to monitor the status of the SSL VPN tunnel. SSA reports real-time and historical events.
- SysMonitor: The SysMonitor application displays operating information about the SSL VPN tunnel. It can capture the information to log files for analysis. Use this tool to collect information only when requested by technical support personnel.
- Fault reporting: The SSL VPN service generates faults for its own components when problems occur. You can set event filters so that you receive notifications when these faults occur, and you can configure the destination where notifications are sent. For information about how to set event filters and configure alarm destinations, see Configuring alarm notifications on page 46.

Viewing the tunnel status

Use the following procedure to view the status of the SSL VPN tunnel using the System Status Application (SSA).

Procedure

1. Launch SSA using one of the following methods:
   - Launch SSA from the IP Office Admin DVD.
   - Select **Start > Programs > IP Office > System Status**.
   - From within Manager, select **File > Advanced > System Status**.
2. Select **IP Networking > SSL VPN** from the navigation list.
   A summary table lists information about each SSL VPN service that is configured.
3. To view detailed information about a specific SSL VPN service, highlight the SSL VPN service and click **Select**.
   A detailed table displays status information about the selected SSL VPN service.

Related topics:

Tunnel status field descriptions: summary table on page 70
Tunnel status field descriptions: detail table on page 70

Tunnel status field descriptions: summary table

System Status Application (SSA) displays the following summary information for the SSL VPN service:

Value	Description
Name	The name of the SSL VPN service configured in IP Office.
Service Status	Indicates whether the SSL VPN is in-service or in fallback.
Last Connection Time	The timestamp of the last successful connection.
Last Disconnection Time	The timestamp of the last disconnection.
Tunnel IP Address	The IP address of the SSL VPN tunnel.
Total Missed Heartbeats	A cumulative count of missed heartbeat signals. The count resets to 0 when you reboot IP Office, or if you de-provision the SSL VPN service in Manager.
Total Missed Keepalives	Keepalives are used for UDP connections. UDP is not supported for the SSL VPN service; the value is 0.
Local TCP Endpoint	The TCP IP address and port number of IP Office.
Remote TCP Endpoint	This is the public address and port number of the AVG. The VIP of the AVG.
Local UDP Endpoint	UDP is not supported for the SSL VPN service; the value is 0.
Remote UDP Endpoint	UDP is not supported for the SSL VPN service; the value is 0.

Tunnel status field descriptions: detail table

System Status Application (SSA) displays the following details for the SSL VPN service:

Value	Description
Service name	The name of the service configured in IP Office.
Service status	Indicates whether the SSL VPN is in-service or in fallback.
Account name	The account name of the SSL VPN service. This account name is used for authenticating the SSL VPN service when connecting with the AVG.
Server address	The address of the VPN gateway server at the service provider site. The address displayed can be an IPv4 address or a Fully Qualified Domain Name (FQDN) address.
Server type	The SSL VPN service is supported by the Avaya VPN Gateway. The server type is AVG.
Protocol	The protocol used by the SSL VPN service for data transport is TCP. If you select UDP as the protocol when you configure the connection, UDP displays in this field but the SSL VPN service falls back to TCP.
Last date and time connected	The timestamp of the last successful connection.
Last date and time disconnected	The timestamp of the last disconnection.
Tunnel IP address	The IP address of the SSL VPN tunnel.
Tunnel subnet mask	The subnet mask of the SSL VPN tunnel.
Tunnel gateway IP address	The default gateway IP address of IP Office.
Tunnel domain	The domain address of the tunnel.
Local TCP IP address	The TCP IP address of IP Office.
Local TCP port	The TCP port of IP Office. The port number is dynamic.
Remote TCP IP address	The TCP IP address of the AVG server.
Remote TCP port	The TCP port of the AVG server. The default port number is 443.
Local UDP IP address	UDP is not supported for the SSL VPN service; the value is 0.
Local UDP port	UDP is not supported for the SSL VPN service; the value is 0.

Value	Description
Remote UDP IP address	UDP is not supported for the SSL VPN service; the value is 0.
Remote UDP port	UDP is not supported for the SSL VPN service; the value is 0.
Primary DNS	The address of the primary DNS server configured on the AVG. This address is provided for informational purposes and is not used by IP Office.
Secondary DNS	The address of the secondary DNS server configured on the AVG. This address is provided for informational purposes and is not used by IP Office.
Primary WINS	The primary WINS configured on the AVG. This address is provided for informational purposes and is not used by IP Office.
Secondary WINS	The secondary WINS configured on the AVG. This address is provided for informational purposes and is not used by IP Office.
Total Missed Heartbeats	A cumulative count of missed heartbeat signals. The count resets to 0 when you reboot IP Office, or if you de-provision the SSL VPN service in Manager.
Total Missed Keepalives	Keepalives are used for UDP connections. UDP is not supported for the SSL VPN service; the value is 0.

Monitoring alarms using SSA

Use this procedure to view system faults related to the SSL VPN service that are reported in the System Status Application (SSA).

Procedure

1. Launch SSA using one of the following methods:
   - Launch SSA from the IP Office Admin DVD.
   - Select **Start > Programs > IP Office > System Status**.
   - From within Manager, select **File > Advanced > System Status**.

2. Select **Alarms > Service** from the navigation list.
   A table lists the system faults. System faults that are related to the SSL VPN service are identified by the service name.

Related topics:

SSA alarm descriptions on page 73

SSA alarm descriptions

The following system faults are related to the SSL VPN service and are reported in the System Status Application (SSA).

Name	Description
Last Date of Error	The date and time that the alarm occurred.
Occurrences	The number of times that the alarm has occurred since the control unit was last restarted or the alarm was last cleared.
Error Description	The alarms related to the SSL VPN service display the following error messages, followed by the name of the SSL VPN service: • SSL VPN out of service due to planned maintenance • SSL VPN out of service due to server not being reachable or network failure • SSL VPN out of service due to TLS session negotiation failure • SSL VPN out of service due to TLS session key re-negotiation failure • SSL VPN out of service due to lack of resources on IP Office • SSL VPN out of service due to an internal error in IP Office • SSL VPN out of service due to too many missed heartbeat messages • SSL VPN out of service due to failure to resolve server FQDN • SSL VPN out of service due to duplicate IP address detected on another IP Office interface

Name	Description
	• SSL VPN out of service due to authentication failure • SSL VPN out of service due to a SOCKS protocol error • SSL VPN out of service due to the server reporting an error

Troubleshooting the SSL VPN service

You can use information captured by SysMonitor to troubleshoot connectivity issues. SysMonitor captures information that can help to troubleshoot issues when the SSL VPN service does not connect with the AVG and the System Status Application (SSA) does not provide enough information to identify the root cause of the failure.

Use this procedure to collect information only when requested by technical support personnel.

Procedure

1. Select **Start > Programs > IP Office > Monitor**.
   The SysMonitor application connects to the IP Office server and displays a system log.
2. Select **Filters > Trace** options and click the **VPN** tab.
3. In the SSL VPN area, select the filters specified by technical support.
4. Click **OK**
   The SysMonitor log lists the activity for the SSL VPN service under the name that you configured for the service.

Related topics:

SysMonitor output descriptions on page 74

SysMonitor output descriptions

The following table lists the filters that you can select in SysMonitor, and describes outputs that each filter generates. This information is intended for technical support personnel when troubleshooting the SSL VPN service.

Name	Description
Configuration	Displays information about when the SSLVPN service was added, modified, or deleted.
Session	Displays information about the status of the SSL VPN service, such as whether the tunnel is in service or in fallback, or trying to connect. When the SSL VPN service is connected, this shows the negotiated SSL VPN tunnel parameters with AVG.
SessionState	Displays information about the state when an event occurs. The defined states are: Idle, Connecting, Connected, Disconnecting, WaitingToStart, and NeedsRestart.
Fsm	Used for UDP connections. UDP is not supported for the SSL VPN service; no output is generated.
Socks	Displays the SOCKS stack events triggered by signalling messages.
SocksState	Displays the internal states of the SOCKS stack when SOCKS5 signalling messages are processed.
Heartbeat	Displays information about when heartbeat messages are sent and received.
Keepalive	Used for UDP connections. UDP is not supported for the SSL VPN service; no output is generated.
SignalingPktRx	Displays a byte stream of SOCKS signaling packets received from the AVG.
SignalingPktTx	Displays a byte stream of SOCKS signaling packets sent to the AVG.
DataPktRx	Displays a subset of the datagram, beginning with the data packet received by the SSL VPN tunnel from AVG and passed on to the IP Office system.
DataPktTx	Displays a subset of the datagram, beginning with the data packet sent by the SSL VPN tunnel interface to the AVG.
TunnelInterface	Displays information about the interactions between the SSL VPN tunnel interface and the IP Office IP stack.

Name	Description
TunnelRoutes	Displays information about the split tunneling routes installed in and removed from the IP Office routing table.

Chapter 11: Maintaining the SSL VPN service

This section describes the tasks that you perform on an on-going basis after the SSL VPN service is configured and connected.

Use the information in this section to perform the following maintenance tasks:

- taking the tunnel out-of-service and restoring it to service
- changing the password for the SSL VPN account

Enabling and disabling the service

After you configure the SSL VPN service, you can use the following interfaces to enable or disable the tunnel.

- Manager
- System Status Application (SSA)
- short codes dialed on Avaya deskphones
- programmable keys on supported Avaya deskphones
- an auto-attendant configured on Embedded Voicemail or Voicemail Pro systems
- set-based administration on supported Avaya deskphones

The methods available depend on the operating mode that you use.

The following table lists the methods supported in each operating mode:

Method	Operating mode			
	Essential Edition	IP Office Server Edition	Server Edition Expansion System	Basic Edition
Manager	✔	✔	✔	—
SSA	✔	✔	✔	—

Method	Operating mode			
	Essential Edition	IP Office Server Edition	Server Edition Expansion System	Basic Edition
Shortcodes dialled on Avaya deskphones	✔	✔	✔	—
Programmable keys on Avaya deskphones	✔	✔	✔	—
Auto-attendant on Embedded Voicemail or Voicemail Pro systems	✔	✔	✔	—
Set-based administration	—	—	—	✔

Related topics:

Enabling the service using Manager on page 78
Disabling the service using Manager on page 79
Enabling the service using SSA on page 79
Disabling the service using SSA on page 80
Enabling the service using a short code on page 80
Disabling the service using a short code on page 81
Enabling and disabling the service using set-based administration on page 81
Enabling and disabling the service using programmable keys on page 82

Enabling the service using Manager

Use this procedure to enable the SSL VPN service from the Manager interface. If you are configuring a Server Edition system, use IP Office Manager for Server Edition mode.

The SSL VPN service must have a status of In Fallback before you begin.

Procedure

1. In the navigation list, right-click **Service**.
   The list expands to display the services configured on the system.
2. Select the SSL VPN service that you want to enable.
3. Select the **Fallback** tab and de-select the **In Fallback** option.
4. Click **OK**.

5. Click the **Save** icon to save the configuration.

Disabling the service using Manager

Use this procedure to disable the SSL VPN service from the Manager interface. If you are configuring a Server Edition system, use IP Office Manager for Server Edition mode.

The SSL VPN service must have a status of In Service before you begin.

Procedure

1. In the navigation list, right-click **Service**.
   The list expands to display the services configured on the system.
2. Select the SSL VPN service that you want to disable.
3. Select the **Fallback** tab and select the **In Fallback** option.
4. Click **OK**.
5. Click the **Save** icon to save the configuration.

Enabling the service using SSA

Use this procedure to enable the SSL VPN service from the System Status Application (SSA) . The SSL VPN service must have a status of In Fallback before you begin.

Procedure

1. Launch SSA using one of the following methods:
   - Launch SSA from the IP Office Admin DVD.
   - Select **Start > Programs > IP Office > System Status**.
   - From within Manager, select **File > Advanced > System Status**.
2. Select **IP Networking > SSL VPN** from the navigation list.
3. Select the SSL VPN service that you wish to enable from the list.
4. Click the **Set in Service** button.
   The status changes to In Service.

Disabling the service using SSA

Use this procedure to disable the SSL VPN service from the System Status Application (SSA) . The SSL VPN service must have a status of In Service before you begin.

Procedure

1. Launch SSA using one of the following methods:
   - Launch SSA from the IP Office Admin DVD.
   - Select **Start > Programs > IP Office > System Status**.
   - From within Manager or IP Office Manager for Server Edition, select **File > Advanced > System Status**.
2. Select **IP Networking > SSL VPN** from the navigation list.
3. Select the SSL VPN service that you wish to enable from the list.
4. Click the **Set in Fallback** button.
   A confirmation dialog box displays.
5. Click **Yes**.
   The system generates an alarm to confirm that the SSL VPN service is disabled.
6. To view the alarm, select **Alarms > Service** from the navigation list.
   The alarm displays the following message: “SSL VPN put of service due to planned maintenance” followed by the name of the service.

Enabling the service using a short code

Use this procedure to enable the SSL VPN service by dialling a short code from a deskphone. The SSL VPN service must have a status of In Fallback before you begin.

Before you begin

This feature is available only if the system administrator has configured short codes on the IP Office system. For more information, see Configuring short codes on page 42. Before you begin, you must know the number that the system administrator has configured in the short code to identify the SSL VPN service.

Procedure

From a deskphone connected to the IP Office system, enter ***775*x*1**, where *x* represents an instance of the SSL VPN service, ranging from 1 to 9. For example, if

the system administrator has configured the short code so that **1** identifies the SSL VPN service, enter ***77511**.
The SSL VPN connection is placed in service.

Disabling the service using a short code

Use this procedure to disable the SSL VPN service by dialling a short code from a deskphone. The SSL VPN service must have a status of In Service before you begin.

Before you begin

This feature is available only if the system administrator has configured short codes on the IP Office system. For more information, see Configuring short codes on page 42. Before you begin, you must know the number that the system administrator has configured in the short code to identify the SSL VPN service.

Procedure

From a deskphone connected to the IP Office system, enter ***775*x*0**, where *x* represents an instance of the SSL VPN service, ranging from 1 to 9. For example, if the system administrator has configured the short code so that **1** identifies the SSL VPN service, enter ***77510**.
The SSL VPN connection is placed in fallback.

Enabling and disabling the service using set-based administration

On some models of Avaya phones, you can use softkeys to enable and disable the SSL VPN service. This section provides information about this feature and the phones that support it.

Before you begin

You must configure System Phone Rights for the user before this feature is available. For information about how to set System Phone Rights, see *IP Office Manager*.

The phones must be plugged into the one of the first two ports of the first card on the IP500 V2 platform.

About this task

You can use softkeys to enable and disable the SSL VPN service on the following Avaya phones:

- ETR 18D and ETR 34D Deskphones
- 1416 Digital Deskphone

- 1408 Digital Deskphone
- 9504 Digital Deskphones
- 9508, Digital Deskphones
- T7316 and 7316E Digital Deskphones
- M7310 and M7324 Digital Deskphones

The following procedure provides a general guide to accessing the SSL VPN feature on these phones. For detailed information about menu options, refer to the user guide for your phone.

Procedure

1. The menus that you need to navigate to access the SSL VPN feature depend on the model of phone that you use. Use one of the following methods to access the SSL VPN feature:
   - Select **Admin > System Administration > System Parameters** and scroll to locate the SSL VPN Service.
   - Select **Admin > Feature** and scroll to locate the SSL VPN Service.
   - Select **Admin** and press **#775** to access the SSL VPN menu.
2. Press the appropriate softkey to enable or disable the service.

Enabling and disabling the service using programmable keys

Some models of Avaya phones provide programmable keys. You can use these keys as a short cut so that you do not need to enter a feature code or navigate through menus on the phone interface in order to activate a feature. Your system administrator can configure a programmable key that allows you to enable and disable the SSL VPN service.

If your system administrator has configured a programmable key on your phone for the SSL VPN service, a label displays next to the programmed key on your phone.

Press the key to toggle the SSL VPN service between enabled (in service) and disabled (in fallback).

The status of the SSL VPN service displays next to the key on the phone. The way in which the status displays depends on the model of the phone. For example, some phones display an icon, and others use LEDs to indicate the status of a feature. When the icon displays or the LED lights, the SSL VPN service is enabled.

When you press the key to disable the SSL VPN service, the icon is no longer displayed and the LED turns off.

Resetting the password

This section describes the methods that you can use to reset the password for the SSL VPN service.

There are two methods of resetting the password of the SSL VPN service.

- You can change the password in the on-boarding file and re-import it.
- You can change the password using Manager.

For both methods, you must also change the password that is configured for the SSL VPN service on the RADIUS server.

Related topics:

Resetting the password using an on-boarding file on page 83
Resetting the password using Manager on page 84

Resetting the password using an on-boarding file

Use this procedure when you have already configured the SSL VPN service on an IP Office system and need to modify the password for the SSL VPN service.

Perform this procedure from the Avaya IP Office Web Manager interface at the customer site.

Before you begin

Before you begin, you must have the following information:

- the SSL VPN service name
- the account name used for authenticating the SSL VPN service when connecting with the AVG.

You can use the System Status Application (SSA) to find the SSL VPN service name and the account name. For more information, see Viewing the tunnel status on page 69.

You must also reset the password for the SSL VPN service on the RADIUS server.

Procedure

1. Select **Tools > On-boarding**.
   The On-boarding dialog box displays.
2. Click **Modify**.
   A browser opens and navigates to the Avaya web site.
3. Log in to the web site.

The IP Office Remote Connectivity / Password Management page displays.

4. Click **Existing IP Office SSL VPN Remote Connectivity**.
5. Select **Password Reset**.
   The default SSL VPN service name displays.
6. Ensure that service name that is displayed matches the name of the SSL VPN service for which you want to reset the password. If the default service name does not match, enter the service name,
7. Enter the SSL VPN account name.
8. Click **Submit**.
9. Select whether you want to receive the updated on-boarding file by email, or whether you want to download the updated file and follow the prompts on the screen.
10. When you have either downloaded or received the updated on-boarding file, save it to your local system.
11. Browse to the location where you saved the on-boarding file and click **Upload** on the Web Manager interface.
    A message displays to confirm that the on-boarding file has installed successfully.

Next steps

After you have reset the password, confirm that the SSL VPN service has successfully reconnected with AVG by following the procedure Viewing the tunnel status on page 69.

Resetting the password using Manager

Use this procedure to modify the password for the SSL VPN service. Perform this procedure from the Manager interface at the customer site. If you are configuring a Server Edition system, use IP Office Manager for Server Edition mode.

Before you begin

You must also reset the password for the SSL VPN service on the RADIUS server.

Procedure

1. In the navigation list, select **Service**.
2. Select the name of the SSL VPN service.
3. Select the **Session** tab and enter the new password for the SSL VPN service account in the **Account password** field.
4. Re-enter the password in the **Confirm password** field.

5. Click **OK**.
6. Click the **Save** icon to save the configuration.

Chapter 12: Appendix A: AVG Quick Setup log file example

```
Alteon iSD SSL
Hardware platform: 3050
Software version: 9.0.0.42
------------------------------------------------------------
[Setup Menu]
      join       - Join an existing cluster
      new        - Initialize host as a new installation
      boot       - Boot menu
      info       - Information menu
      exit       - Exit  [global command, always available]

>> Setup# new

Setup will guide you through the initial configuration.

Enter port number for the management interface [1-4]: 1
Enter IP address for this machine (on management interface): 172.16.1.4
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Setup a two armed configuration (yes/no) [no]: yes
Enter port number for the traffic interface [1-4]: 2
Enter IP address for this machine (on traffic interface): 216.13.56.90
Enter network mask [255.255.255.224]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Enter default gateway IP address (on the traffic interface): 216.13.56.65
Enter the Management IP (MIP) address: 172.16.1.5
Making sure the MIP does not exist...
Enter a timezone or 'UTC' or 'select' [select]:
Timezone setting
 1 - Africa
 2 - Americas
 3 - Antarctica
 4 - Arctic Ocean
 5 - Asia
 6 - Atlantic Ocean
 7 - Australia
 8 - Europe
 9 - Indian Ocean
10 - Pacific Ocean
Select a continent or ocean: 2
Countries:
 1 - Anguilla           18 - Ecuador            35 - Paraguay
 2 - Antigua & Barbuda  19 - El Salvador        36 - Peru
 3 - Argentina          20 - French Guiana      37 - Puerto Rico
 4 - Aruba              21 - Greenland          38 - St Barthelemy
 5 - Bahamas            22 - Grenada            39 - St Kitts & Nevis
 6 - Barbados           23 - Guadeloupe         40 - St Lucia
 7 - Belize             24 - Guatemala          41 - St Martin (French
 8 - Bolivia            25 - Guyana             42 - St Pierre & Mique
 9 - Brazil             26 - Haiti              43 - St Vincent
10 - Canada             27 - Honduras           44 - Suriname
11 - Cayman Islands     28 - Jamaica            45 - Trinidad & Tobago
```

```
12 - Chile              29 - Martinique         46 - Turks & Caicos Is
13 - Colombia           30 - Mexico             47 - United States
14 - Costa Rica         31 - Montserrat         48 - Uruguay
15 - Cuba               32 - Netherlands Antil  49 - Venezuela
16 - Dominica           33 - Nicaragua          50 - Virgin Islands (U
17 - Dominican Republi  34 - Panama             51 - Virgin Islands (U
Select a country: 47
Regions:
 1 - Adak Aleutian Islands
 2 - Anchorage Alaska Time
 3 - Boise Mountain Time - south Idaho & east Oregon
 4 - Chicago Central Time
 5 - Denver Mountain Time
 6 - Detroit Eastern Time - Michigan - most locations
 7 - Honolulu Hawaii
 8 - Indiana/Indianapolis Eastern Time - Indiana - most locations
 9 - Indiana/Knox Eastern Time - Indiana - Starke County
10 - Indiana/Marengo Eastern Time - Indiana - Crawford County
11 - Indiana/Petersburg Central Time - Indiana - Pike County
12 - Indiana/Tell_City Central Time - Indiana - Perry County
13 - Indiana/Vevay Eastern Time - Indiana - Switzerland County
14 - Indiana/Vincennes Eastern Time - Indiana - Daviess, Dubois, Knox & Mart
15 - Indiana/Winamac Eastern Time - Indiana - Pulaski County
16 - Juneau Alaska Time - Alaska panhandle
17 - Kentucky/Louisville Eastern Time - Kentucky - Louisville area
18 - Kentucky/Monticello Eastern Time - Kentucky - Wayne County
19 - Los_Angeles Pacific Time
20 - Menominee Central Time - Michigan - Dickinson, Gogebic, Iron & Menomine
21 - New_York Eastern Time
22 - Nome Alaska Time - west Alaska
23 - North_Dakota/Center Central Time - North Dakota - Oliver County
24 - North_Dakota/New_Salem Central Time - North Dakota - Morton County (exc
25 - Phoenix Mountain Standard Time - Arizona
26 - Shiprock Mountain Time - Navajo
27 - Yakutat Alaska Time - Alaska panhandle neck
Select a region: 21
Selected timezone: America/New_York
Enter the current date (YYYY-MM-DD) [2012-09-06]:
Enter the current time (HH:MM:SS) [12:14:58]:
Enter NTP server address (or blank to skip):
Enter DNS server address: 10.1.1.100
Generate new SSH host keys (yes/no) [yes]:
This may take a few seconds...ok
Enter a password for the "admin" user:
Re-enter to confirm:
Run VPN quick setup wizard [yes]:
  Creating default networks under /cfg/vpn 1/aaa/network
  Creating default services under /cfg/vpn 1/aaa/service
Enter VPN Portal IP address: 216.13.56.91
Is this VPN device used in combination with an Alteon switch? [no]:
Enter comma separated DNS search list
  (eg company.com,intranet.company.com): avaya.com,support.avaya.com
Create HTTP to HTTPS redirect server [yes]:
Create a trusted portal account [yes]:
User name: carmen
User password:
  Creating group 'trusted' with secure access.
  Creating user 'carmen' in group 'trusted'.
  Creating empty portal linkset 'base-links' for group trusted.
Setup IPsec [no]:
Initializing system......ok
Setup successful. Relogin to configure
```

Chapter 13: Appendix B: Modifying the default AVG for SSL VPN (with screens)

After running the Quick Setup and Net Direct configuration wizards, the default configuration must be modified to support an SSL VPN connection with an IP Office system.

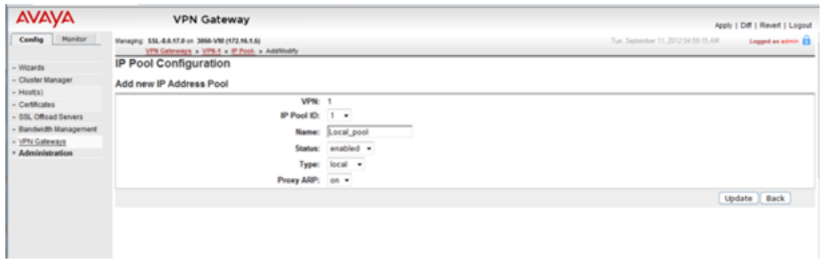
Perform this procedure using the AVG browser-based interface (BBI). See *Avaya VPN Gateway BBI Application Guide*.

Before you begin

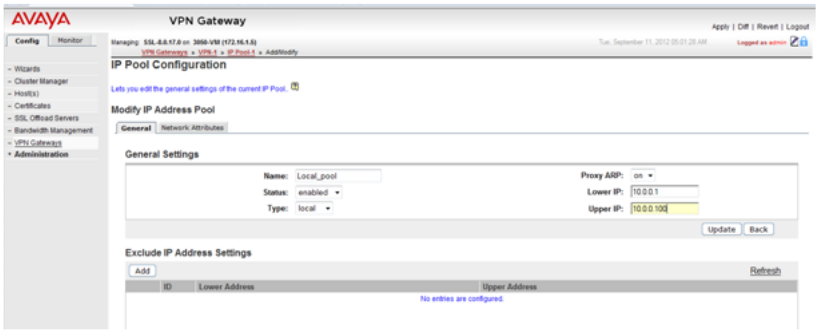
Ensure that the default gateway configuring on AVG responds to ICMP requests. If the default gateway does not respond to ICMP requests, the AVG cannot provide VPN services.

Procedure

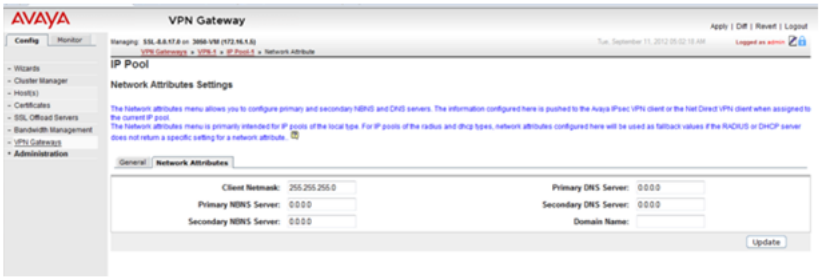
1. Log on to the AVG BBI as administrator.
2. In the navigation pane on the left, select the **Config** tab and then **VPN Gateway** > **VPN1** > **IP Pool**.
3. The default VPN from the basic AVG configuration may already have a local pool. If not, you must add a local pool to the default VPN. On the **Add new IP Address Pool** page, add a local pool to the default VPN.



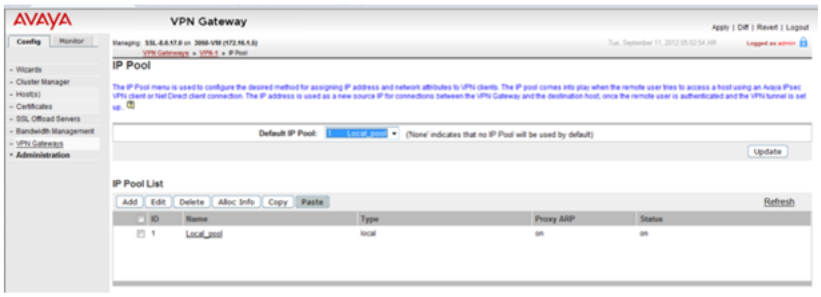
4. On the **Modify IP Address Pool** page, verify that the values in the **Lower IP** and **Upper IP** fields match values set using the Net Direct Configuration wizard.



5. On the **IP Pool** > **Network Attributes Settings** page, select the **Network Attributes** tab and enter the values for your network.

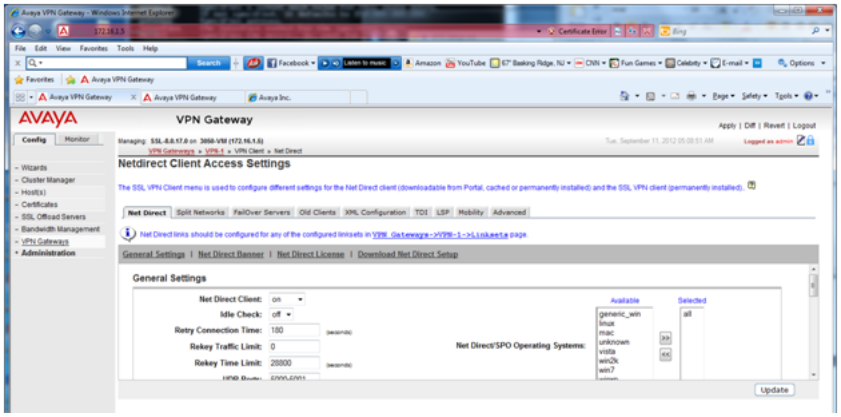


6. On the **IP Pool** page, set the **Default IP Pool** to the local poll created in step 3.

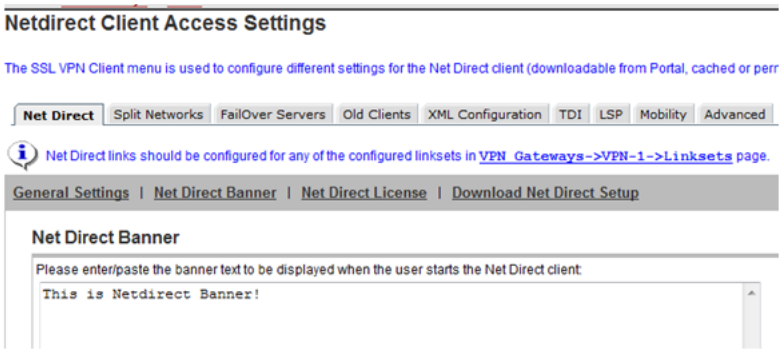


7. On the **Net Direct Client Access Settings** page, verify the settings created by the Net Direct Configuration wizard.

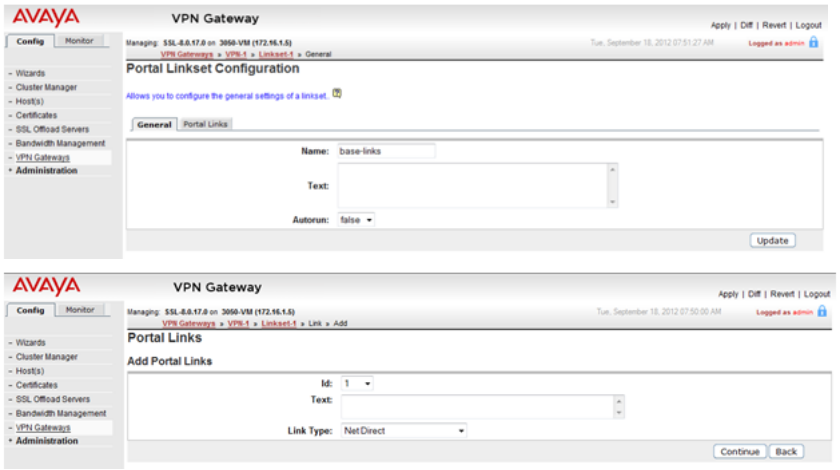
   a. Ensure that **Idle Check** is set to **off**.



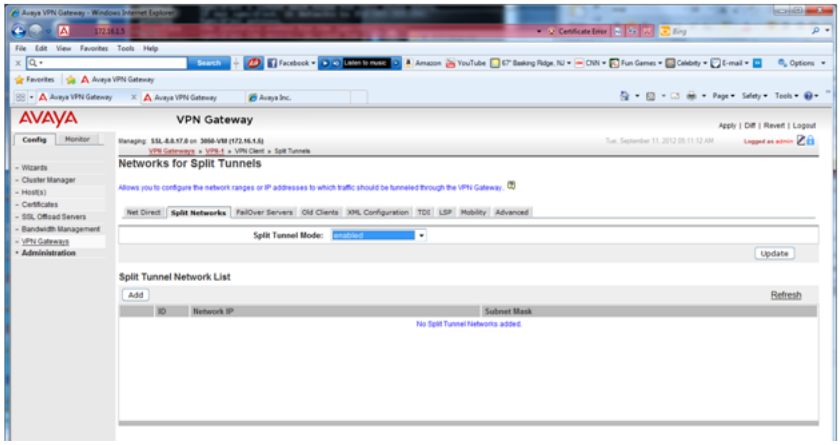
b. Ensure that the Net Direct Banner is set.



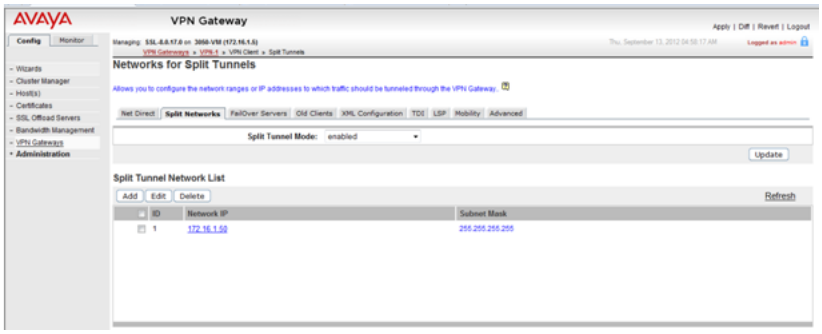
8. Set the portal link for launching the Net Direct client. On the **Portal Linkset Configuration** page, Select the **Portal Link** tab. In the **Link Type** field, select **Net Direct**.



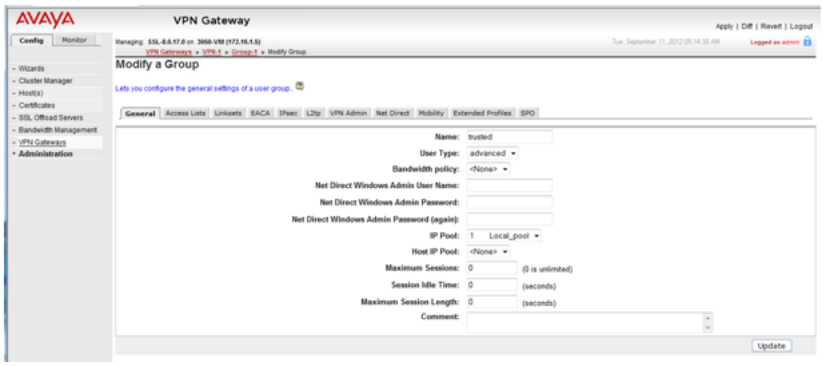
9. On the **Networks for Split Tunnels** page:
   a. Set **Split Tunnel Mode** to **enabled**.



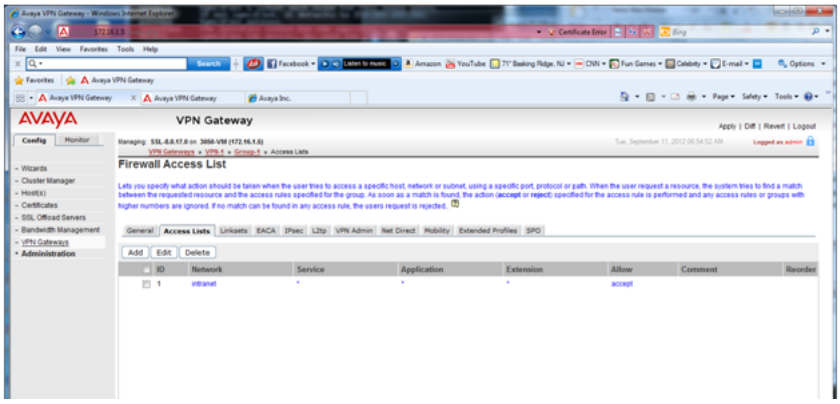
b. Set the split tunneling routes to reach the service agent on the private network.



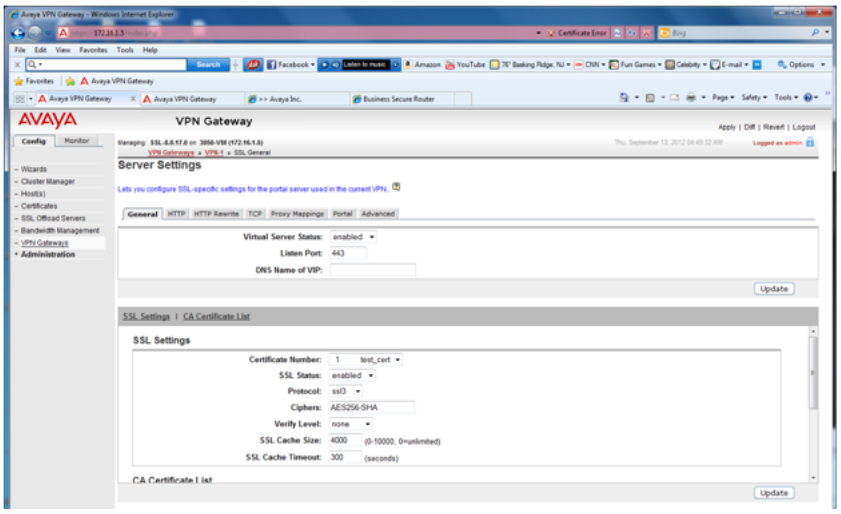
10. For VPN1, go to the groups page and select **Group1**. On the **Modify a Group** page, set the IP Pool to the local pool created in step 3.



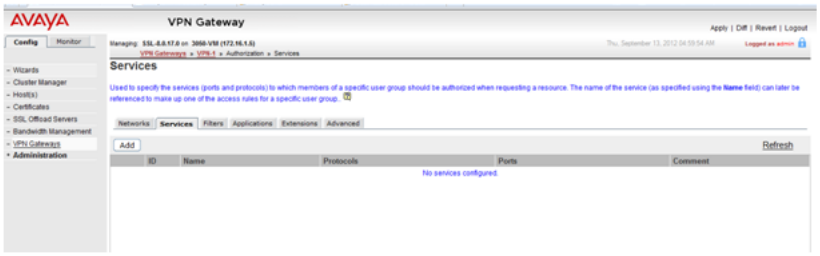
11. Go to the **VPN1** > **Group1** > **Access Lists** page. On the **Firewall Access List** page, create an access rule if it was not created by default.



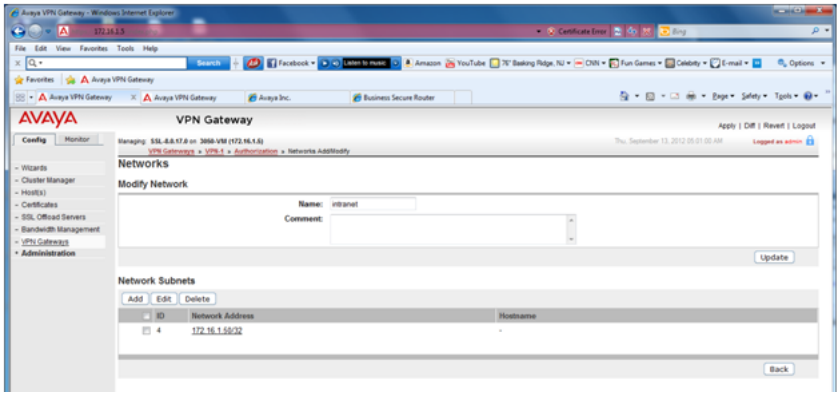
12. Go to the **VPN1** > **SSL** page. On the **Server Settings** page, under **SSL Settings** set **Ciphers** to **AES256-SHA** for a strong encryption.



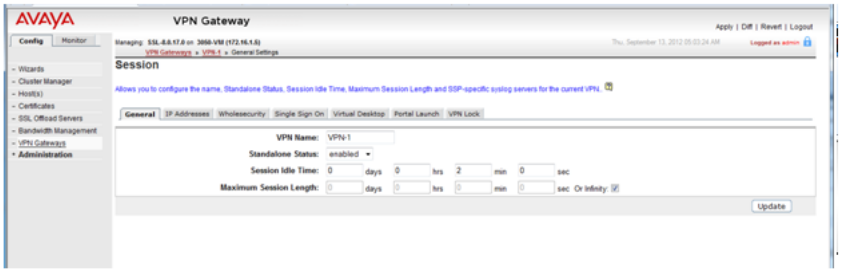
13. Go to the **VPN1** > **Authorization** > **Services** page. Remove all the services set in the default configuration as they are not required by SSL VPN.



14. Go to the **VPN1** > **Authorization** > **Networks** page. Set the authorization network subnet that is referenced in one of the access rules that is set under **VPN1** > **Group1** > **Access Lists**.



15. Go to the **VPN1** > **General Settings** > **Session** page. Set **Session Idle Time** to 2 minutes.



Chapter 14: Appendix C: Configuring RADIUS authentication (with screens)

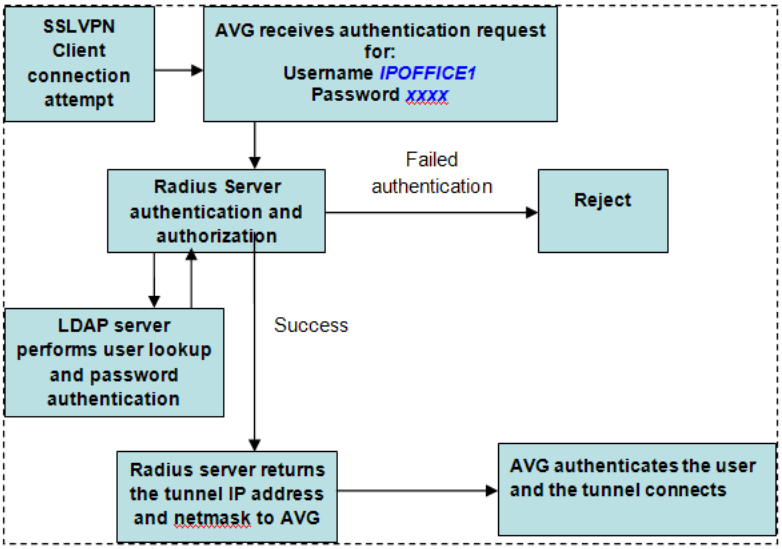
The key benefit of RADIUS authentication is that the SSL VPN service is always assigned the same tunnel IP address.

To configure RADIUS authentication, you must install a RADIUS server. Avaya recommends the Avaya Identity Engine for a Radius Server. For information and software download, go to http://support.avaya.com.

RADIUS protocol authentication information such as user account information as well as SSL VPN tunnel information such as IP address and netmask need to be stored in a database. There are two possible options:

- Use Identity Engine's local database to store the user information and provide both lookup and authentication and authorization services. This option can be used for a small number of users. Identity Engine has a hard limit of users. Consult the documentation for the exact value.
- Use an LDAP server to store user credentials and SSL VPN tunnel information for both lookup and authentication services. This option fits deployment scenarios for a large number of users.

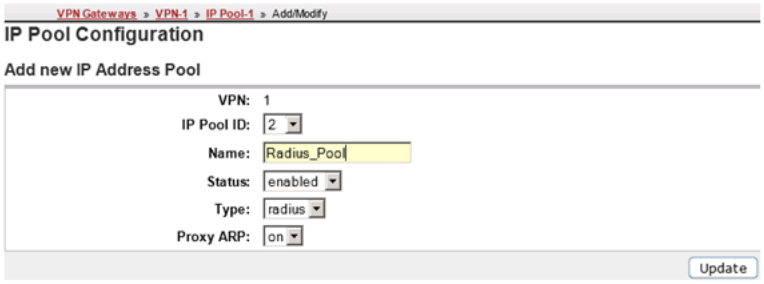
For LDAP server installation, Avaya Identity Engine Radius Server documentation contains configuration options for LDAP servers from different vendors. RADIUS authentication using an LDAP server is illustrated in the figure below. Note that this RADIUS server configuration in this procedure does not require an LDAP server.



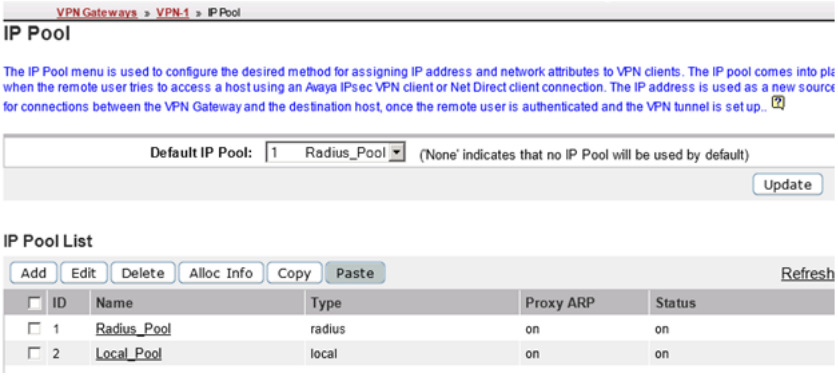
This procedure covers the manual steps to configure RADIUS authentication. Alternatively, you can configure authentication using the AVG authentication wizard.

Procedure

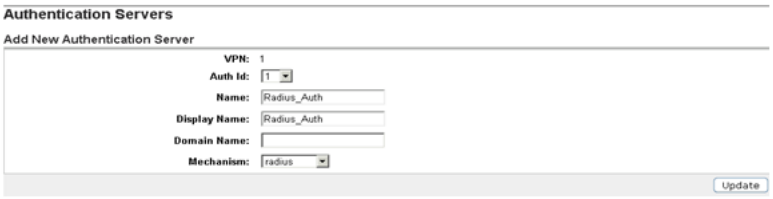
1. Log on to the AVG BBI as administrator.
2. On the **IP Pool Configuration** page, add a new IP Address Pool for RADIUS authentication.



3. On the **IP Pool** page, set the **Default IP Pool** to the RADIUS authentication IP address pool you created in step 2.

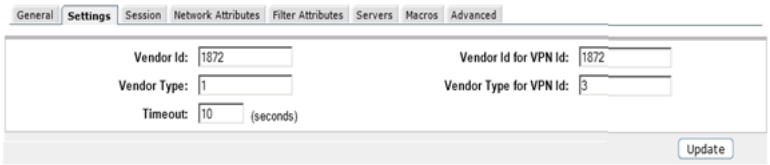


4. Modify the VPN. On the **Authentication Servers** > **Add New Authentication Server** page, complete the fields for the RADIUS server.



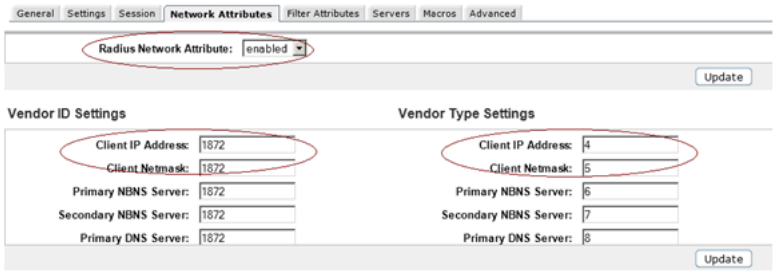
5. Configure the RADIUS authentication server settings. Note that Vendor Id 1872 is associated to vendor Alteon and identifies AVG. Select the **Settings** tab and complete the following fields.

   - **Vendor ID: 1872**
   - **Vendor Type: 1**
   - **Timeout: 10**
   - **Vendor Id for VPN Id: 1872**
   - **Vendor Type for VPN Id: 3**



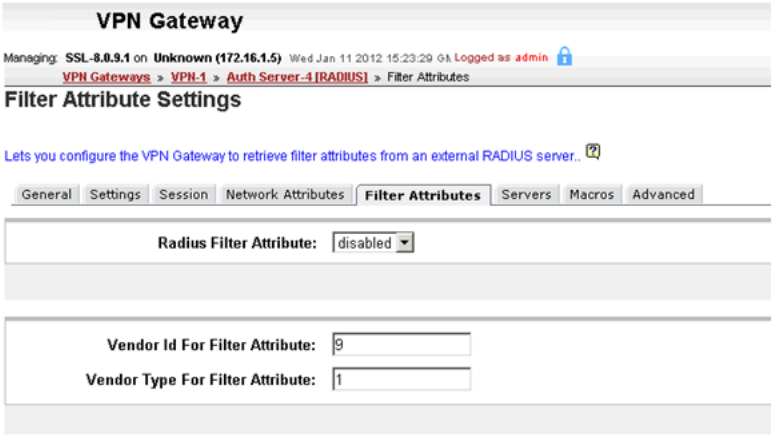
6. Configure RADIUS network attributes. Select the **Network Attributes** tab and complete the following fields.

Vendor ID Settings	Vendor Type Settings
Client IP Address: 1872	Client IP Address: 4
Client Netmask: 1872	Client Netmask: 5
Primary NBNS Server: 1872	Primary NBNS Server: 6
Secondary NBNS Server: 1872	Secondary NBNS Server: 7
Primary DNS Server: 1872	Primary DNS Server: 8



7. Configure filter attributes. Select the Filter Attributes tab and complete the following fields>.

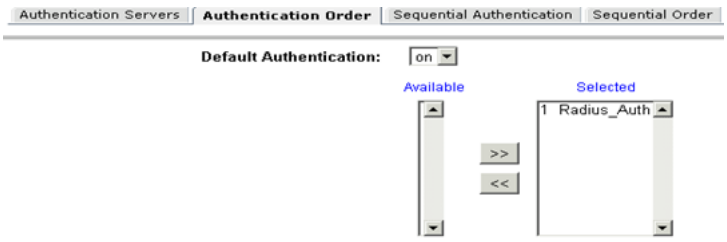
- **Radius filter attribute: disabled**
- **Vendor Id for Filter Attribute: 9**
- **Vendor Type for Filter Attribute: 1**



8. Specify the Radius server address. Select the **Servers** tab on the **RADIUS Servers** page.

9. Click **Add** and on the **Modify RADIUS Server** page, enter the RADIUS server IP address and shared secret.

10. Select the **Authentication Order** tab and specify the preferred order for authentication methods.


Authentication Servers
Authentication Order
Sequential Authentication
Sequential Order
Default Authentication:
on
Available
Selected
1 Radius_Auth
>>
<<

Chapter 15: Appendix D: AVG configuration settings

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

>> Main# cfg

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

>> Configuration# dump
Dump private/secret keys (yes/no) [no]:
Collecting data, please wait...
/*
/*
/* Alteon iSD SSL
/* Configuration dump taken Tue Sep 18 08:40:50 EDT 2012
/* Hardware Platform: 3050-VM
/* Software Version: 8.0.17.0
/* Uptime:  8 days 3 hours 59 minutes
/* IP Address: 172.16.1.4
/* Hardware Address: 00:0c:29:e0:d8:73
/* Disk space:   config         10110  386513  3 %
  user_content   32832  6015488  1 %

/*
/*
/cfg/.
/cfg/ssl/.
/cfg/ssl/server 1/.
        name "Redirect to VPN 1"
        vips 216.13.56.91
        standalone off
        port "80 (http)"
        rip 0.0.0.0
```

```
        rport 81
        type http
        proxy on
        loopback on
        fastfin off
        ena enabled
/cfg/ssl/server 1/trace/.
/cfg/ssl/server 1/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        verify none
        log none
        verifylog none
        ciphers ALL:-EXPORT:-LOW!ADH
        ena disabled
/cfg/ssl/server 1/tcp/.
        cwrite 15m
        ckeep 15m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/ssl/server 1/http/.
        httpsredir on
        redirect on
        downstatus unavailable
        securecookie off
        certcard off
        cookieonce off
        sslheader on
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addfront off
        addbeassl off
        addbeacli off
        addclicert off
        addnostore off
        nocachehdr off
        compress off
        cmsie on
        rhost off
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/ssl/server 1/http/redirmap/.
/cfg/ssl/server 1/http/dynheader/.
/cfg/ssl/server 1/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
/cfg/ssl/server 1/http/auth/.
        mode basic
        realm Xnet
```

```
        proxy off
        ena disabled
/cfg/ssl/server 1/dns/.
/cfg/ssl/server 1/adv/.
/cfg/ssl/server 1/adv/pool/.
        timeout 15s
        ena disabled
/cfg/ssl/server 1/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/.
        type all
        persistence none
        metric hash
        health auto
        interval 10s
        grace on
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/script/.
/cfg/ssl/server 1/adv/loadbalancing/remotessl/.
        protocol ssl3
        ciphers ALL
/cfg/ssl/server 1/adv/loadbalancing/remotessl/verify/.
        verify none
/cfg/ssl/server 1/adv/sslconnect/.
        protocol ssl3
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
        ena disabled
/cfg/ssl/server 1/adv/sslconnect/verify/.
        verify none
/cfg/cert 1/.
        name test_cert
        cert
-----BEGIN CERTIFICATE-----
MIIEejCCA+OgAwIBAgIJAODDyCE7V9E3MA0GCSqGSIb3DQEBBAUAMIG/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEQMA4GA1UEBxMHVGVzdGluZzEo
MCYGA1UEChMfVGVzdCBJbmMuIDEgMDQ6Mzc6MjEgMjAxMi0wOS0xMDESMBAGA1UE
CxMJdGVzdCBkZXB0MSAwHgYDVQQDExd3d3cuZHVtbXlzc2x0ZXN0aW5nLmNvbTEp
MCcGCSqGSIb3DQEJARYadGVzdGVyQGR1bW15c3NsdGVzdGluZy5jb20wHhcNMTIw
OTEwMDgzNzIyWhcNMTMwOTEwMDgzNzIyWjCBvzELMAkGA1UEBhMCVVMxEzARBgNV
BAgTCkNhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3Qg
SW5jLiAxIDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEg
MB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEW
GnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCyw80A6VzNwFRpizR9iWJnvZziAgwJZBmI7V2QjtQD+7tMwZA1mNZf
JohYRRS24WGOerGJd3YtAkQHv3yWSo6NiQ5X0Ng8ou4wvg7nlhsqSjeReSn7RUPV
Jl7L45MySiLI5iKWH2j+i1NxLfLbtkqO7+RVAlM3lL4T0Lsjg4RiswIDAQABo4IB
ejCCAXYwDAYDVR0TBAUwAwEB/zARBglghkgBhvhCAQEEBAMCAkQwMgYJYIZIAYb4
QgENBCUWI0FsdGVvbi9Ob3J0ZWwgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1Ud
DgQWBBSGR0w74d4NpcyEeYyLayjiBtRc9DCB9AYDVR0jBIHsMIHpgBSGR0w74d4N
pcyEeYyLayjiBtRc9KGBxaSBwjCBvzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3QgSW5jLiAx
IDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UE
AxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3Rl
ckBkdW1teXNzbHRlc3RpbmcuY29tggkA4MPIITtX0TcwCQYDVR0SBAIwADANBgkq
hkiG9w0BAQQFAAOBgQAMw7vnW4aWgwQZEpjWEYxzRkbAD1+vWYbtdNix9kPtHzWu
e5Fr9c4iuzSHW6cC8natTQc+8iAUNjokBpZ2PT62mENRsNjfj2Ov3/OzXuUYtwkt
OtOCddd5gMlDL6ovxM4k59VLkDYdn5p0kwknSAGHJyoUjQ3g7XWGAOffJy+Wbw==
-----END CERTIFICATE-----
...
```

```
/cfg/cert 1/revoke/.
/cfg/cert 1/revoke/automatic/.
        anonymous false
        interval 1d
        verify off
        ena disabled
/cfg/vpn 1/.
        name VPN-1
        ips 216.13.56.91
        standalone on
        hostippool false
/cfg/vpn 1/aaa/.
        idlettl 2m
        sessionttl infinity
        authorder 1
        defauth on
        defippool 1
/cfg/vpn 1/aaa/tg/.
        ena disabled
        recheck 15m
        action teardown
        details on
        runonce off
        logmode off
        loglevel info
        bypass off
/cfg/vpn 1/aaa/tg/agent/.
        timeout 2s
        minver 0.0.0.0
/cfg/vpn 1/aaa/nap/.
        autorem false
/cfg/vpn 1/aaa/nap/probation/.
        ena false
/cfg/vpn 1/aaa/nap/servers/.
/cfg/vpn 1/aaa/nap/shvs/.
        add 311 128 wshv
        add 40082 0 nshv
/cfg/vpn 1/aaa/nap/wshv/.
        firewall on
        autoupdate on
/cfg/vpn 1/aaa/nap/wshv/virus/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/spyware/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/secupdates/.
        enabled false
/cfg/vpn 1/aaa/wholesec/.
        ena false
/cfg/vpn 1/aaa/auth 1/.
        type local
        name local
/cfg/vpn 1/aaa/auth 1/local/.
        pwdage 0
        expirewarn 15
/cfg/vpn 1/aaa/auth 1/adv/.
/cfg/vpn 1/aaa/seqauth/.
        ena false
        copyuser off
        usesecond off
        retries 3
/cfg/vpn 1/aaa/network 1/.
        name intranet
/cfg/vpn 1/aaa/network 1/subnet 4/.
        net 172.16.1.50
        mask 255.255.255.255
```

```
/cfg/vpn 1/aaa/group 1/.
        name trusted
        restrict 0
        usertype advanced
        idlettl 0
        sessionttl 0
        ippool 1
/cfg/vpn 1/aaa/group 1/access 1/.
        network intranet
        service *
        appspec *
        extspec *
        action accept
/cfg/vpn 1/aaa/group 1/linkset/.
        add base-links
/cfg/vpn 1/aaa/group 1/l2tp/.
/cfg/vpn 1/aaa/group 1/ipsec/.
/cfg/vpn 1/aaa/ssodomains/.
/cfg/vpn 1/aaa/ssoheaders/.
/cfg/vpn 1/aaa/radacct/.
        ena false
/cfg/vpn 1/aaa/radacct/servers/.
/cfg/vpn 1/aaa/radacct/vpnattribute/.
        vendorid "1872 (alteon)"
        vendortype 3
/cfg/vpn 1/aaa/adv/.
/cfg/vpn 1/aaa/adv/unmatchgrp/.
        ena disabled
/cfg/vpn 1/server/.
        port "443 (https)"
        loopback on
        fastfin off
        ena enabled
/cfg/vpn 1/server/trace/.
/cfg/vpn 1/server/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        log none
        verifylog none
        ciphers AES256-SHA
        verify none
        ena enabled
/cfg/vpn 1/server/tcp/.
        cwrite 15m
        ckeep 15m
        skeep 2m
        sinterval 1m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/vpn 1/server/http/.
        downstatus unavailable
        securecookie on
        certcard off
        cookieonce off
        sslheader off
        sslxheader off
        sslsidheader off
        addxfor off
```

```
        addvia on
        addxisd off
        addclicert off
        addnostore on
        nocachehdr off
        compress off
        allowimage on
        allowdoc off
        allowscript off
        allowica on
        cmsie on
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/vpn 1/server/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
/cfg/vpn 1/server/proxymap/.
/cfg/vpn 1/server/portal/.
        wipecookies on
        cookiedb on
        resetcookie off
        persistent off
/cfg/vpn 1/server/portal/urlrewrite/.
        rewrite on
        jrewrite on
        cssrewrite on
        gziprewrite on
        ena enabled
/cfg/vpn 1/server/adv/.
/cfg/vpn 1/server/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/vpn 1/server/adv/sslconnect/.
        protocol ssl23
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
/cfg/vpn 1/server/adv/sslconnect/verify/.
        verify none
/cfg/vpn 1/l2tp/.
        ena disabled
        cert unset
        authorder mschapv2,pap
        groupmatch true
/cfg/vpn 1/ipsec/.
        ena disabled
        cert unset
        groupmatch true
        groupbind off
/cfg/vpn 1/ipsec/sys/.
/cfg/vpn 1/ipsec/sys/failover/.
        primary 0.0.0.0
        secondary 0.0.0.0
        tertiary 0.0.0.0
/cfg/vpn 1/ipsec/sys/nat-t/.
        udpport 10001
```

```
        portswitch off
        ena false
/cfg/vpn 1/ippool 1/.
        type local
        name Local_pool
        lowerip 10.0.0.1
        upperip 10.0.0.100
        proxyarp on
        ena enabled
/cfg/vpn 1/ippool 1/exclude/.
/cfg/vpn 1/ippool 1/netattr/.
        netmask 255.255.255.0
        primnbns 0.0.0.0
        secnbns 0.0.0.0
        primdns 0.0.0.0
        secdns 0.0.0.0
/cfg/vpn 1/portal/.
        logintext
This is a configurable text.
...
        seclogtext
This is a configurable text.
...
        iconmode fancy
        linktext

...
        linkurl on
        punblock off
        linkcols 2
        linkwidth 100%
        companyname "Avaya Inc."
        smbworkgrp WORKGROUP
        autojre on
        applet on
        wiper on
        rsaauto off
        ieclear on
        citrix off
        clientauth off
        trustsite off
/cfg/vpn 1/portal/colors/.
        color1 #ececec
        color2 #ececec
        color3 #cc0000
        color4 #cc0000
/cfg/vpn 1/portal/content/.
        ena disabled
/cfg/vpn 1/portal/faccess/.
        ena disabled
        ipsecmode native
        contip 0.0.0.0
        portalmsg
From this page you can gain full network access. This
requires that Net Direct is enabled or
that you have either Avaya's IPSEC client (version 4.89 or better)
and/or SSL-VPN (TDI version 1.1 or better) client installed. If the Net Direct
installable client is installed it will be used if Net Direct is enabled.
Note: Your browser must support Java. If not download SUN's
J2SE JRE from
class="white_link" href="javascript:download_jre()">www.java.com.
Remember: You can only access resources on the network as defined by
your access rights. Contact your network operator if you are
dissatisfied with your current access rights.
...
```

```
appletmsg
The quest for full network access has started._The outcome of the quest will be indicated in
the progress bar and console window below.
...
/cfg/vpn 1/portal/lang/.
        setlang en
/cfg/vpn 1/portal/lang/beconv/.
/cfg/vpn 1/portal/whitelist/.
        ena disabled
/cfg/vpn 1/portal/whitelist/domains/.
/cfg/vpn 1/portal/blacklist/.
        ena disabled
/cfg/vpn 1/portal/blacklist/domains/.
/cfg/vpn 1/portal/usertype/.
/cfg/vpn 1/portal/usertype/novice/.
        sysinfo off
/cfg/vpn 1/linkset 1/.
        name base-links
        autorun false
/cfg/vpn 1/linkset 1/link 1/.
        href <netdirect>
        NetdirectFlag off
        type netdirect
/cfg/vpn 1/linkset 1/link 1/netdirect/.
/cfg/vpn 1/vdesktop/.
        ena off
        prelogon off
        always off
        force off
        switch off
        secure off
        persist off
        filesep off
        remdisk off
        print off
        netshare off
        cryptlevel 128
        timeout 5
        conncntrl off
/cfg/vpn 1/vdesktop/mcd/.
        ena disabled
        keylogger off
        scrscrap off
        acntcreate off
/cfg/vpn 1/vdesktop/mcd/vkeyboard/.
        ena disabled
/cfg/vpn 1/sslclient/.
        ippool off
        netdirect on
        caching off
        ndbanner
This is Netdirect Banner!
...
ndlicense
END USER LICENSE AGREEMENT
FOR AVAYA VPN CLIENT
This Software License Agreement ('Agreement') is between you, ('User') and Avaya Corporation
and its subsidiaries and affiliates ('Avaya').  PLEASE READ THE FOLLOWING CAREFULLY.
BY CLICKING ON THE 'YES' BUTTON OR USING THIS SOFTWARE, YOU ('USER') ARE CONSENTING TO BE BOUND
BY THIS AGREEMENT BETWEEN YOURSELF AND AVAYA.  IF YOU DO NOT AGREE TO BE BOUND BY THIS
AGREEMENT, CLICK 'NO' AND DO NOT USE THIS SOFTWARE.
LICENSE GRANT: This Agreement shall govern the licensing of Avaya and Avaya licensor's
software and the accompanying user manuals, on line help services, Avaya Web Site and other
instructions (collectively, the 'Software') provided or made available to User.  The Software
includes client software, which resides on the computers of User, to access Sublicensor's
```

```
networks (the 'Client Software').  The Software provided under this License is proprietary to
Avaya and to third parties from whom Avaya has acquired license rights.  This Software was
licensed in conjunction with the purchase of a 'Avaya VPN Gateway' or other Avaya VPN device,
that will give the User access to the Sublicensor's purchaser's network and may only be used
for this purpose by you.  User is hereby granted a nonexclusive object code only license to
use the Software under the following terms:
- User shall use the Software only in conjunction with the Avaya VPN Gateway or other Avaya
VPN device with which the Software was distributed.
- User may make one copy of the Software only for safekeeping (archives) or backup purposes.
- User may not modify, translate, adapt, decompile, disassemble, decrypt, extract, or
otherwise reverse engineer or attempt to discover the source code and techniques incorporated
in the Software.  User may not create derivative works based on the Software or any trade
secret or proprietary information of Avaya.
- Title to Software shall not pass to User.
- User shall not provide, or otherwise make available, any Software, in whole or in part, in
any form, to any third party, nor shall User sublicense, rent or lease the Software.
- Upon termination or breach of this Agreement, or in the event that the Avaya device with
which it was distributed is no longer in use, User will immediately cease use of  and destroy
all copies of the Software and  return the Software to Avaya or certify as to such destruction
to Avaya that is has been destroyed. Avaya and Third-party owners from whom Avaya has acquired
license rights to material that is incorporated into the Software shall have the right to
enforce the provisions of this Agreement against User. IN NO EVENT SHALL AVAYA OR ITS  AGENTS,
SUPPLIERS, MANUFACTURERS OR DISTRIBUTORS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING,
WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF
BUSINESS INFORMATION OR DATA, DAMAGES BASED ON ANY THIRD PARTY CLAIM,  OR, OR ANY OTHER
PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF SUCH PARTY HAS
BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.  SOME JURISDICTIONS DO NOT ALLOW THESE
LIMITATIONS OR EXCLUSIONS AND IN SUCH EVENT THEY MAY NOT APPLY.
User agrees to comply with all export restrictions regarding the Software, and shall not
export, directly or indirectly, any Software or related technical data or information without
first obtaining any required export licenses or other governmental approvals. THE SOFTWARE IS
PROVIDED 'AS IS' WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED,
INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF
THE SOFTWARE REMAINS WITH USER.  Avaya is not obligated to User to provide support of any kind
for the Software, and in the event it chooses to do so, such support is subject to the terms
of this Agreement.  Some jurisdictions do not allow exclusion of implied warranties and, in
such event, the above exclusions may not apply. If User is the United States Government, the
following paragraph shall apply:  All Software provided hereunder is commercial computer
software and commercial computer software documentation, as applicable, and in the event
Software is licensed for or on behalf of the United States Government, the respective rights
to the Software is governed by Avaya standard commercial license in accordance with U.S.
Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and  48 C.F.R.
227.7202 (for DoD entities). Software contains trade secrets and copyrighted material and User
agrees to treat the Software as confidential information using a reasonable standard of care.
User shall not remove or obscure any copyright, patent, trademark, trade secret, or similar
intellectual property or restricted rights notice within or affixed to any Software and shall
reproduce and affix such notices on any backup copy of software. User may terminate this
Agreement at any time.  Avaya may terminate this Agreement if User fails to comply with any
of its terms.  This Agreement is the complete and exclusive agreement between the parties
hereto regarding its subject matter, and shall be governed solely by the laws of the state of
New York, without regard to its rules governing conflicts of law.
...
          oslist all
        udpports 5000-5001
        rekeytraf 0
        rekeytime 8h
        portalbind on
        idlecheck off
        keepalive 0
        recncttime 3m
        clampmss on
        splittun enabled
        tdiclient off
        lspclient off
```

```
        oldclients false
/cfg/vp
```

Index

A

alarm destinations 46–49
  about 46
  email notifications 48
  SNMP traps 47
  syslog entries 49
alarms 46, 55, 72, 73
  about 46
  monitoring SSA 72
  SSA descriptions 73
  testing 55
architecture 13
auto attendant 44
AVG 20, 22–24, 54, 101
  configuration settings 101
  configuring 22
  modifying the default configuration 24
  remote access 23
  task flow 20
  testing 54

C

certificates 41
  installing 41
configuring 50
  static routes 50
connectivity 74
  troubleshooting 74

D

disabling SSL VPN 43, 77, 79–82
  about 77
  Manager 79
  programmable keys 82
  short codes 43, 81
  SSA 80
document changes 7
documentation 16

E

email 48
  alarm destinations 48
enabling SSL VPN 43, 44, 77–80, 82
  about 77
  auto attendant 44
  Manager 78
  programmable keys 82
  short codes 43, 80
  SSA 79

F

fault management 47–49, 55, 72, 73
  email notifications 48
  SNMP trap destinations 47
  SSA alarm descriptions 73
  SSA alarms, monitoring 72
  syslog entries 49
  test alarms 55
features 9

I

infrastructure 19, 29
  about 19
  configure RADIUS server 29
integration 89
  configuring AVG 89
IP routing 50
  static routes 50

M

Manager 39, 78, 79
  configuring SSL VPN service 39
  disabling SSL VPN 79
  enabling SSL VPN 78
monitoring 57, 69
  IP Office system 57
  remote 57
  tunnel status 69

N

NAPT 52
  delete rule 52

O

on-boarding 34
configuring SSL VPN 34
existing instances 34

P

password 83, 84
reset using Manager 84
reset using on-boarding 83

Q

Quick Setup 87
log file 87

R

remote access 57–63
about 57
Manager 61
Manager for Server Edition 62
NAPT 60
SSA 58
SysMonitor 59
Web Control for Server Edition 63
Web Manager 60
remote upgrades 67
requirements 15

S

security 41
Installing certificates 41
service provider 19
site configuration 19
short codes 42, 80, 81
configuring 42
using to disable 81
using to enable 80
SNMP traps 47
destinations 47
SSA 55, 69, 72, 73, 79, 80
alarm descriptions 73
alarm monitoring 72
disabling SSL VPN 80
enabling SSL VPN 79
test alarms 55
viewing tunnel status 69
SSL VPN service 9, 33, 37, 42, 83
about 9
Avaya service provider 33
password reset 83
short codes 42
third party service provider 37
static routes 50
configuring 50
syslog entries 49
alarm destinations 49
system architecture 13
system requirements 15

T

testing 55
alarms 55
Testing connection 53
troubleshooting 74, 75
SysMonitor outputs 75
using SysMonitor 74
tunnel 69–71, 77
connecting 77
disconnecting 77
status details 71
status summary 70
viewing status 69

U

upgrades 67

V

Verify connection 53, 54
BBI 54
SysMonitor 53

W

workflow 17