Avaya IP Office SSL VPN Solutions Guide

Release 8.1
01.01
June 2012

Notice

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

Documentation disclaimer

"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 Web sites 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 Web site: 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.

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 End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified 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 communicate 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 by Avaya 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). End User 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). Customer 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"). (see "Third-party Components" for more information).

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

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

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 Web site: 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: About the SSL VPN service

About the SSL VPN service

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.

Overview

The SSL VPN service provides an always-on connection to an AVG server. 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

Operating modes

The SSL VPN service is supported on IP500v2 hardware operating in the following modes:

- IP Office Essential Edition
- IP Office 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
- IP Office Basic Edition

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						
	Essential Edition		IP Office Server Edition	Server Edition Expansion System	Basic Edition		Branch mode (IP500 v2)
	IP500	IP500v2			IP500	IP500 v2	
Connectivity							
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	—	—	—	—	—	—	—
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	—	✔	✔	✔	—	✔	—

Supported features	Operating mode						
	Essential Edition		IP Office Server Edition	Server Edition Expansion System	Basic Edition		Branch mode (IP500 v2)
	IP500	IP500v2			IP500	IP500 v2	
Office Manager for Server Edition							
Remote monitoring using System Status Application	—	✔	✔	✔	—	✔	—
Remote monitoring using SysMonitor	—	✔	✔	✔	—	✔	—
Enable and disable the SSL VPN service through shortcodes	—	✔	✔	✔	—	—	—
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	—	✔	✔	✔	—	✔	—

Supported features	Operating mode						
	Essential Edition		IP Office Server Edition	Server Edition Expansion System	Basic Edition		Branch mode (IP500 v2)
	IP500	IP500v2			IP500	IP500 v2	
service using programmable keys on Avaya deskphones							
Remote upgrade of IP Office to new releases	—	✔	✔	✔	—	✔	—

Management and monitoring 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.

Deployment options

When you set up the AVG server, you can choose to set up a one-armed configuration or a two-armed configuration for your deployment. Avaya recommends that you use two-armed configuration. In a two-armed configuration, you configure 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 instances 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 by sending a query to an external RADIUS server. The SSL VPN service is assigned the same IP address and netmask each time that it authenticates with the AVG, based on attributes that you configure when you set up the RADIUS server.

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

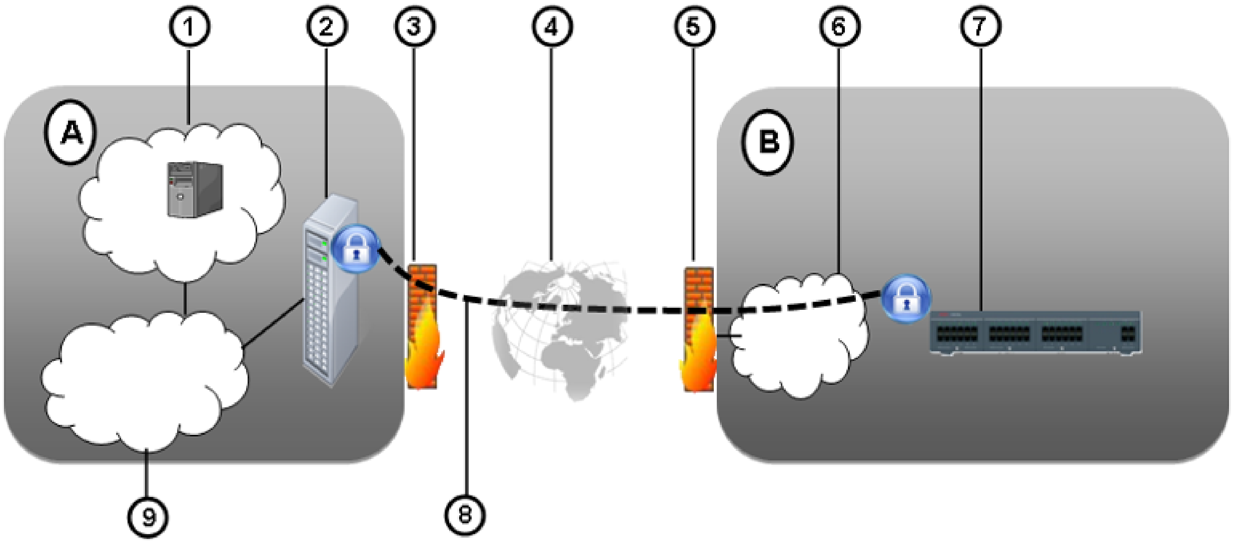
A fault management server is an optional component in the SSL VPN service. You can locate a fault management server at the service provider site and use the SSL VPN service to send system faults to that server. You can set event filters to determine which faults are reported. For example, you can set 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.

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.



Item	Description
A	The service provider site where AVG is installed.

Item	Description
B	The customer site where IP Office and its application servers are installed.
1	The private network at the service provider site. You can install a service agent, an authentication server, and a fault management server on this private network.
2	The AVG where the VPN is configured.
3	The service provider firewall.
4	The internet.
5	The customer firewall.
6	The private network at the customer site, which includes the WAN and corporate router.
7	The IP Office system where the SSL VPN is configured. The connection of the SSL VPN tunnel is initiated at the customer site.
8	The solution uses a secure SSL/TLS control channel to authenticate the username and password of the SSL VPN service. This connection is used for both signaling and data transport over TCP.
9	The private network at the service provider site that is connected to the AVG. You can install a service agent, an authentication server, and a fault management server on this private network.

System requirements and limitations

Requirements

The SSL VPN solution has the following 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 The SSL VPN service requires a RADIUS server to ensure that the SSL VPN tunnel is assigned the same IP address each time that it authenticates with the Avaya VPN Gateway (AVG. 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	SSL VPN Service does not require a license key

Limitations

The SSL VPN solution has the following 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.

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 2: Configuring the infrastructure

Configuring the infrastructure

This section provides information about the tasks that you must complete when you install and configure an Avaya VPN Gateway (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 provides an overview of the configuration tasks that you must complete, as well as procedures for configuring the interoperation of the AVG with an IP Office system.

Related topics:

Infrastructure tasks on page 15
Configuring certificates in AVG on page 18
Disabling idle checking on page 20
Configuring the session idle time on page 20
RADIUS settings on page 21

Infrastructure tasks

This section provides an overview of the procedures that you must perform at the service provider site.

Use the following table to understand the tasks that you must perform when you configure the infrastructure for the SSL VPN service. To complete these tasks, you need to refer to the documentation suite for the Avaya VPN Gateway (AVG), as well as to the documentation provided by other vendors to support the hardware and software used in your network infrastructure.

#	Task	Description	Refer to . . .
1	Set up the AVG server	Set up a server that is equipped with the following: • one network interface card (NIC) if you are creating a one-armed configuration • two NICs if you are creating a two-armed configuration (recommended) Assign a static IP address to each NIC.	Documentation provided by the equipment vendor
2	Install the AVG on a server or on a virtual machine	Choose one of the following options: • Install the AVG on a server and allow the installation process to format the hard drive and create partitions. • Install the AVG on a virtual machine.	*VMWare Getting Started Guide for Avaya VPN Gateway* (46120–302)
3	Set up and initialize the AVG	The setup menu displays and guides you through configuring the AVG.	"Intial Setup" in the *Avaya VPN Gateway User Guide* (NN46120–104)
4	Configure certificates	Configure AVG so that it requires certificates to authenticate clients.	"Certificates and Client Authentication" in the *Avaya VPN Gateway User Guide* (NN46120–104) For information about certificate requirements for the SSL VPN service, see Configuring certificates in AVG on page 18
5	Configure remote access	To allow administrators to connect and configure the VPN gateway remotely, enable the following remote access services: • SSH • HTTPS	Avaya VPN Gateway BBI Application Guide (NN46120–102) or Avaya Command Line Interface (CLI) Application Guide (NN46120–101) and Avaya Command Reference (NN46120–103)

#	Task	Description	Refer to . . .
6	Set the default gateway to the public internet and configure static routes	Add static routes so that Net Direct clients can reach service agents located on the private intranet at the service provider site.	Avaya Command Line Interface (CLI) Application Guide (NN46120–101) and Avaya Command Reference (NN46120–103)
7	Create and configure a VPN	You need a single VPN instance for all IP Office systems to connect. When you create a VPN instance, you configure a portal IP address for the VPN; the SSL VPN service uses this portal IP address to connect. Use the broswer-based interface (BBI) or CLI commands to configure the VPN.	Avaya VPN Gateway BBI Application Guide (NN46120–102) and Managing users and groups in the Avaya VPN Gateway User Guide (NN46120–104). or Avaya Command Line Interface (CLI) Application Guide (NN46120–101) and Avaya Command Reference (NN46120–103)
	Add a new VPN		
	Enable the standalone status		
	Set the IP pool configuration		
	Add link sets and a portal link for NetDirect Client		
	Configure authorization		
	Configure groups		
	Configure authentication to use a RADIUS server		
	Enable Net Direct		
	Configure the split network ranges or IP addresses to which traffic should be tunneled through the VPN gateway		
8	Configure system integration	Configure these settings to optimize the interoperation between the AVG and IP Office.	Configuring the session idle time on page 20 Disabling idle checking on page 20
9	Set up the service provider server	Locate this server on the intranet on the private side of the AVG and set up the static IP address and static routes for this server. You can use this server for authentication and fault management services.	Documentation provided by the equipment vendor

#	Task	Description	Refer to . . .
10	Set up RADIUS server	The SSL VPN service requires a RADIUS server. Avaya recommends that you use the Avaya Identity Engines Ignition Server as the RADIUS server.	If you are using the Identity Engines Ignition Server as the RADIUS server, refer to the *Avaya Identity Engines Ignition Server — Configuration Guide* (NN47280-500). Otherwise, refer to the documentation provided by the RADIUS server vendor. For a list of attributes that you must configure for the SSL VPN service, see RADIUS settings on page 21.
11	Configure a fault management server	Optional. If you configure a fault management server, you must configure the SNMP Agent Device ID name. Avaya recommends that you set the SSL VPN service Account Name to match the SNMP Agent Device ID name.	Documentation provided by the equipment vendor
12	Configure the router	Configure corporate routing between the AVG and its private network. If your corporate router is already configured to allow HTTPS traffic, the SSL VPN service works transparently through the firewall without further configuration.	Documentation provided by the equipment vendor

Configuring certificates in AVG

This section describes the requirements that digital certificates must meet in order to establish an SSL VPN connection between IP Office and the Avaya VPN Gateway (AVG) server.

Use the information in this table to ensure that the certificate installed in the AVG meet the requirements for the SSL VPN service.

For information about how to manage certificates in AVG, see *Avaya VPN Gateway User Guide* (NN46120-104).

Certificate type	Requirements
All certificates	The certificate must be a valid X.509 v3 certificate with valid X.509 v1 fields. The minimum fields required are: • version • serial number • signature algorithm • issuer • valid from • valid To • subject • public Key • thumbprint algorithm • thumbprint
	The certificate must have a date that is within the interval defined in the Valid from, and Valid To fields.
	The RSA key size must be between 1024 and 4096 bits. Note: Due to the fact that the key length is processed according to the number of bytes, a minimum key length between 1017 and 1023 bits is valid because it is rounded to 1024, a multiple of 8.
	The AVG certificate must not match the IP Office identity certificate.
	The certificate must be part of a valid chain to a trusted root CA.
	The certificate must have a valid RSA public key algorithm and a valid thumbprint.
Self-signed certificate (a single certificate signed by itself)	If a self-signed certificate is used by the AVG server, it must be installed in the IP Office Trusted Certificate store.
Single CA signed certificate (a leaf certificate directly signed by root CA)	The root CA that signed the AVG certificate must be installed in the IP Office Trusted Certificate store.
	The actual AVG certificate does not need to be installed in the IP Office Trusted Certificate store.

Chained CA signed certificate (a leaf certificate signed by an intermediate CA that in turn is signed by a root CA)	The intermediate CA certificate must be installed in the IP Office Trusted Certificate store.
	The actual AVG certificate does not need to be installed in the IP Office Trusted Certificate store.

Disabling idle checking

Use this procedure to configure the settings so that SSL VPN service can access the Avaya VPN Gateway (AVG) and provide an always-on connection. When you disable idle checking, the SSL VPN service is not terminated after a period of inactivity.

Perform this procedure using the AVG browser-based interface (BBI).

Before you begin

You must log in as an administrator to perform this procedure.

Procedure

1. Click on **Config** tab.
2. Select **VPN Gateways** from the navigation list.
3. Click on the VPN gateway name.
4. Click on **VPN Client** settings.
5. On the **Net Direct** tab, select **Off** from the **Idle Check** list.

Configuring the session idle time

Use this procedure to set the period during which a VPN session can be idle before the connection is automatically closed. You must configure this setting so that the resources of the Avaya VPN Gateway (AVG) are properly allocated for the SSL VPN service. When you set the idle time to the minimum, licenses for the SSL VPN service are released more quickly in the event that the connection is lost.

Perform this procedure using the AVG browser-based interface (BBI).

Before you begin

You must log in as an administrator to perform this procedure.

Procedure

1. In the System tree view, select **VPN Gateways**.
2. Select the name of the VPN Gateway that you are using for the SSL VPN service.
3. On the **General** tab, set the **Session Idle Time** to 2 minutes.

RADIUS settings

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.

When you configure a user group on the RADIUS server, configure the following attributes:

Attribute	Type	Description
User-Password	Check	Enter the password for the SSL VPN service account.
Class	Reply IPoffice	Configure this attribute to match the group name on AVG.
Framed-IP-Address	success-Reply	Configure this attribute to assign a static IP address.
Framed-IP-Netmask	success-Reply	Configure this attribute to assign a netmask.

Setting these attributes ensures that the SSL VPN service is assigned the same IP address and netmask each time that it authenticates with the AVG.

Chapter 3: Configuring the IP Office system

Configuring the IP Office system

When you configure the SSL VPN service, it provides an always-on connection between IP Office and an Avaya VPN Gateway (AVG) server installed at the service provider site. After the AVG at the service provider site is configured, you must configure the IP Office system that is installed at a customer site. This section provides information about the configuration process for IP Office.

Configuration tasks

The table below provides an overview of the configuration tasks that you perform on each IP Office system where you want to support an SSL VPN service. It indicates which tasks are required in order to establish an SSL VPN connection with AVG, and which tasks are optional.

Task	Required	Optional
Upgrade IP Office to Release 8.1	✔	—
Configure the DNS server ✱ **Note:** Required only when the SSL VPN service uses an FQDN address.	✔	—
Configure the SSL VPN service using one of the following methods • import an on-boarding XML file using Web Manager • configure the settings using Manager or IP Office Manager for Server Edition and install the security certificate	✔	—
Configure short codes	—	✔
Configure programmable keys	—	✔
Configure static routes	—	✔

Task	Required	Optional
Configure alarm notifications	—	✔
Verify the connection	✔	—
Send a test alarm	—	✔

Configuration methods

There are two ways to configure the SSL VPN service on the IP Office system:

- import an on-boarding XML file using Web Manager
- configure the SSL VPN settings using Manager

If you are using Basic Edition mode to operate your IP Office system, you must import the on-boarding XML file to configure the SSL VPN service.

If you are using Essential Edition or Server Edition mode, you can choose between importing an on-boarding XML file or configuring the settings using Manager. You can update the configuration settings for SSL VPN service using either method; however, it is important to understand the impact of switching between methods before you make updates to the SSL VPN service. The sections below describe each of the configuration methods.

Using the on-boarding XML file:

The on-boarding XML file is available from your service provider. 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 the TLS certificate automatically.

The on-boarding XML file overwrites any settings that already exist for the SSL VPN service. For example, if you configure the SSL VPN service using Manager, and then update the settings using an on-boarding XML file, the settings in the on-boarding XML file will overwrite the settings that you configured in Manager.

Configuring the settings using Manager:

You can use Manager to configure the settings needed to establish a secure tunnel between IP Office and an AVG server. If you are deploying a Server Edition system, you can configure the SSL VPN service by selecting IP Office Manager for Server Edition mode when you launch Manager. The configuration process is the same in both Manager and IP Office Manager for Server Edition mode.

When you use Manager to configure the initial settings for the SSL VPN service, you must also install the TLS certificate.

You can also use Manager to update settings that were imported by an on-boarding XML file. The Manager interface displays the current settings for the SSL VPN service, allowing you to choose the specific settings that you want to modify.

Synchronizing data:

If you switch between methods when you configure and update the SSL VPN service, you must ensure that you synchronize your configuration data before you apply the changes. For example, if you configure settings using Manager, and subsequently import an on-boarding

XML file, the modifications that you made in Manager are overwritten by the settings in the imported file. If you want to maintain the modifications that you made in Manager, you must ensure that the XML file contains the modified settings.

Synchronizing data is particularly important if you have made changes to the password for the SSL VPN service. The password is one of the settings included in the on-boarding XML file. If you change the password in Manager, and subsequently import an on-boarding XML file, the current password is overwritten by the one configured in the on-boarding XML file. If the password configured in the on-boarding file is not synchronized with the current password, the SSL VPN service is not able to reconnect.

Supported modes:

The following table lists the configuration methods supported in each operating mode.

Configuration method	Operating mode			
	Essential Edition	IP Office Server Edition	Server Edition Expansion System	Basic Edition
On-boarding using Web Manager	✔	✔	✔	✔
Manual configuration using Manager or IP Office Manager for Server Edition	✔	✔	✔	—

For information about how to use each configuration method, see Using an on-boarding file to configure the service on page 25 and Using Manager to configure the service on page 29.

Multiple instances

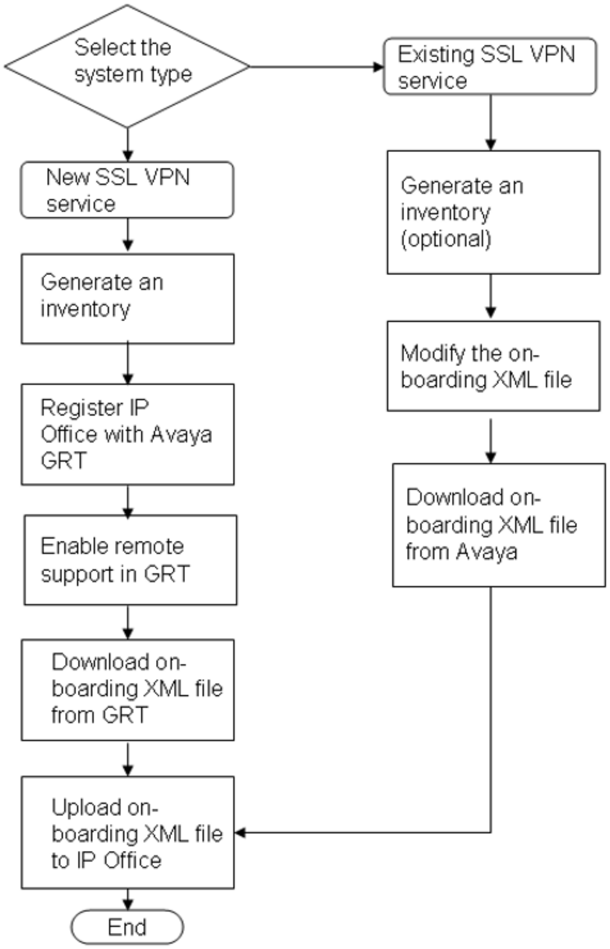
You can configure multiple instances of the SSL VPN service and run them concurrently.

Using an on-boarding file to configure the service

This section provides an overview of the on-boarding process. The process that you follow depends on whether you are configuring a new instance of the SSL VPN service, or whether you are updating an existing SSL VPN configuration.

The on-boarding process

The following chart outlines the steps in the on-boarding process.


Select the system type
Existing SSL VPN service
New SSL VPN service
Generate an inventory (optional)
Generate an inventory
Modify the on-boarding XML file
Register IP Office with Avaya GRT
Download on-boarding XML file from Avaya
Enable remote support in GRT
Download on-boarding XML file from GRT
Upload on-boarding XML file to IP Office
End

New systems:

Follow the process for new systems when you are configuring an IP Office system that you have not yet registered in the Avaya Global Registration Tool (GRT).

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.

Existing systems:

Follow the process for existing systems in the following circumstances:

- you have already configured an SSL VPN service and need to make configuration updates to it
- you need to change an SSL VPN service password
- you reset the IP Office configuration to its default settings and need to reconfigure the SSL VPN

When you follow the process for an existing system, you can choose to generate an inventory but this step is optional. You are prompted to download the XML on-boarding file from the Avaya web site rather than from the GRT web site.

Related topics:

Importing the on-boarding file to configure a new service on page 27

Using the on-boarding file to modify an existing service on page 27

Importing the on-boarding file to configure a new 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 are configuring the SSL VPN service on an IP Office system.

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.

Using Manager to configure the service

You can use Manager to configure the settings needed to establish a secure tunnel between an IP Office Essential Edition system and an AVG server. Use IP Office Manager for Server Edition to configure an SSL VPN service for Server Edition systems. The configuration process is the same in both Manager and IP Office Manager for Server Edition mode.

Configuration process

When you use Manager to configure the initial settings for the SSL VPN service, you must also install the TLS certificate.

If you used an on-boarding file to configure the initial settings for the SSL VPN service, you can use Manager to update those settings. The Manager interface displays the current settings for the SSL VPN service, allowing you to choose the specific settings that you want to modify. For information about the impact of using both Manager and an on-boarding file to configure the SSL VPN service, see Configuration methods on page 24.

Related topics:

Configuring the SSL VPN service on page 29

Installing the certificate on page 32

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.

About this task

Before you begin, you must configure a DNS server address to resolve FQDNs. For more information, see Configuring the DNS server on page 33.

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.

Next steps

When you use Manager or IP Office Manager for Server Edition to configure the initial settings for the SSL VPN service, you must also install a certificate in the IP Office certificate store. For more information, see Installing the certificate on page 32

Related topics:

Service tab field descriptions on page 30
Session tab field descriptions on page 31

Service tab field descriptions

Use the information in this table to configure the fields on the **Service** tab.

Name	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

Name	Description
	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.

Session tab field descriptions

Use the information in this table to configure the fields on the **Session** tab.

Name	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

Name	Description
	AVG, or when the connection with the AVG is lost. The default is 60 seconds.

Installing the 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.

Follow this procedure only if you configured the SSL VPN service using Manager. If you configured the SSL VPN service using an on-boarding file, you do not need to install a certificate; the on-boarding file installs the certificate automatically. For information about these configuration options, see Configuring the IP Office system on page 23.

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

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

About this task

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.

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 the DNS server

Use this procedure to configure the DNS server. 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.

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

Procedure

1. In the navigation list, click **System** and select the **DNS** tab.
2. Configure the settings listed in the table below.
3. Click **OK**.
4. Click the **Save** icon to save the configuration changes.
   The configuration changes are merged. You do not need to reboot the system for the configuration changes to take effect.

Related topics:
DNS field descriptions on page 34

DNS field descriptions

Use the information in this table to configure the DNS settings.

Name	Description
DNS Server IP Address	Enter the IP address of a DNS server. This is the minimum information required to configure the DNS server. The remaining fields are optional.
Backup DNS Server IP Address	Enter the IP address of a backup DNS server. The default is 0.0.0.0 (no backup).
DNS Domain	Enter the DNS domain. This field can be blank.
WINS Server IP Address	Enter the IP address of your local WINS server. This address is used only in Windows operating systems.
Backup WINS Server IP Address	Enter the IP address of a backup WINS server. The default is 0.0.0.0 (no backup).
WINS scope	Enter the WINS scope. This field can be blank.

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.

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 deskphone 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.

The following table lists the operating modes that support short codes.

Feature	Operating mode			
	Essential Edition	IP Office Server Edition	Server Edition Expansion System	Basic Edition
Configure short codes	✔	✔	✔	—

Related topics:

[Configuring a short code to enable the SSL VPN service](#) on page 35
[Configuring a short code to disable the SSL VPN service](#) on page 36
[Configuring an auto attendant](#) on page 37

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.

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

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 ***775*x*1**, 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 29 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.

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

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 ***775*x*0**, 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 29 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.

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 configure short codes. See Configuring short codes on page 34.

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 38.
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 programmable keys

Some models of Avaya phones provide programmable keys. When you configure a programmable key, it acts 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 the feature. Use this procedure to configure a programmable key that enables and disables 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.

About this task

You can configure a programmable key to enable and disable the SSL VPN service on the following Avaya phones:

- 1400 Series Digital Deskphones
- 1600 Series IP Deskphones
- 4600 Series IP Telephones
- 5400 Digital Telephones
- 5600 IP Telephones
- 6400 Digital Telephones
- 9500 Digital Deskphones
- 9600 Series IP Deskphones

When you configure a programmable key, the status of the assigned feature 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 active.

The following table lists the operating modes that support programmable keys.

Feature	Operating mode			
	Essential Edition	**IP Office Server Edition**	**Server Edition Expansion System**	**Basic Edition**
Configure programmable keys	✔	✔	✔	✔

Procedure

1. In the navigation list, select **User** .
   The list expands to display the users configured on the system.
2. Select a user.
3. Select the key on the deskphone that you want to configure and click **Edit**.
4. In the **Label** field, enter a label for the button, such as SSL.
5. In the **Action** field, click the browse button and select **Advanced > Hunt Group > Set HuntGroup Night Service**.
6. In the **Action Data** field, type the name of the SSL VPN service. Use the same name that you entered when you created the SSL VPN service. Do not use quotation marks around the name of the SSL VPN service.
7. Click **OK** to close the dialog box.
8. Click **OK** on the **Button Programming** tab.

9. Click the **Save** icon to save the configuration changes.
   The assigned user can press the programmed key to toggle the status of the SSL VPN service between enabled (in service) and disabled (in fallback).

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.

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

About this task

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

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

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.

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				

Alarm destination	Operating mode			
	Essential Edition	IP Office Server Edition	Server Edition Expansion System	Basic Edition
Syslog server on a local LAN	✔	✔	✔	—
Syslog server over an SSL VPN tunnel	✔	✔	✔	—

Related topics:

Configuring SNMP trap destinations on page 42
Configuring email alarm notifications on page 47
Configuring syslog entries on page 48

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.

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

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.

Related topics:

SNMP trap descriptions on page 43

SNMP trap descriptions

The SSL VPN service generates faults for its own components when problems occur. The following table lists the faults related to the SSL VPN service that can be reported as SNMP traps.

Name	Description

Fault 1	`Enterprise: ipoGenTraps`
	`Bindings (8)`
	`Binding #1: ipoGTEventStdSeverity.0 *** (int32) warning(6)`
	`Binding #2: ipoGTEventDateTime.0 *** (octets)`
	`Binding #3: ipoGTEventDevID.0 *** (octets)`
	`Binding #4: sysDescr.0 *** (octets)`
	`Binding #5: ipoGTEventReason.0 *** (int32) servicePlannedMaintenance(40)`
	`Binding #6: ipoGTEventData.0 *** (octets)`
	`Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to planned maintenance`
	`Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) No action required`

Fault 2	`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) serviceNetworkDisconnection(41)`
	`Binding #6: ipoGTEventData.0 *** (octets)`

Name	Description
	Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to server not being reachable or network failure Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Check network connectivity with server
Fault 3	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) serviceFailedTlsNegotiation(42) Binding #6: ipoGTEventData.0 *** (octets) Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to TLS session negotiation failure Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Ensure certificates are properly installed and valid. Ensure key length and cipher selection are appropriate
Fault 4	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) serviceFailedTlsRenegotiation(43) Binding #6: ipoGTEventData.0 *** (octets) Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to TLS session key re-negotiation failure Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Ensure certificates are properly installed and valid. Ensure key re-negotiation is enabled on server and compatible with IP Office
Fault 5	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) serviceLackOfResources(44) Binding #6: ipoGTEventData.0 *** (octets) Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to lack of resources on IP Office Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Verify over engineering. Manually restart SSL VPN service. Reboot IP Office or contact support if problem persists

Name	Description

Fault 6	`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) serviceInternalError(45)`
	`Binding #6: ipoGTEventData.0 *** (octets)`
	`Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to an internal error in IP Office`
	`Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Manually restart SSL VPN service. Reboot IP Office or contact support if problem persists`

Fault 7	`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) serviceTooManyMissedHeartbeats(46)`
	`Binding #6: ipoGTEventData.0 *** (octets)`
	`Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to too many missed heartbeat messages`
	`Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Check network connectivity with server`

Fault 8	`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) serviceFailedDnsResolution(47)`
	`Binding #6: ipoGTEventData.0 *** (octets)`
	`Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to failure to resolve server FQDN`
	`Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Make sure DNS is configured on IP Office and FQDN can be resolved`

Fault 9	`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) serviceDuplicateIpAddress(48)`
	`Binding #6: ipoGTEventData.0 *** (octets)`
	`Binding #7: ipoGTEventAlarmDescription.0 ***`

Name	Description
	(octets) SSL VPN []: Out of service due to duplicate IP address detected on another IP Office interface Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Check IP Office interface configuration. Avoid configuring two SSL VPN services with same credential
Fault 10	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) serviceAuthenticationFailure(49) Binding #6: ipoGTEventData.0 *** (octets) Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to authentication failure Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Verify credential on server. Verify configuration on IP Office
Fault 11	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) serviceSslVpnStackProtocolError(50) Binding #6: ipoGTEventData.0 *** (octets) Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to a SOCKS protocol error Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Check server configuration. Manually restart SSL VPN service. Reboot IP Office or contact support if problem persists
Fault 12	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) serviceSslVpnServerReportedError(51) Binding #6: ipoGTEventData.0 *** (octets) Binding #7: ipoGTEventAlarmDescription.0 *** (octets) SSL VPN []: Out of service due to the server reporting an error Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) Check server configuration and resource allocation. Contact support if problem persists

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.

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 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.

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 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.

Verifying the connection using SysMonitor

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

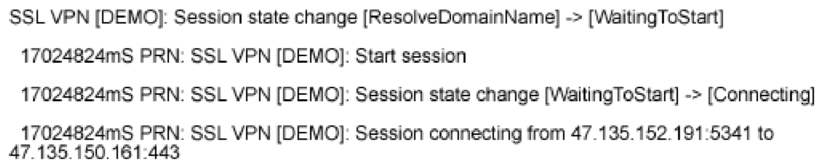
Procedure

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.”

Example

The example below shows a successful connection.



```
SSL VPN [DEMO]: Session state change [ResolveDomainName] -> [WaitingToStart]
  17024824mS PRN: SSL VPN [DEMO]: Start session
  17024824mS PRN: SSL VPN [DEMO]: Session state change [WaitingToStart] -> [Connecting]
  17024824mS PRN: SSL VPN [DEMO]: Session connecting from 47.135.152.191:5341 to
47.135.150.161:443
```

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. For information about alarm destinations and how to define them, see Configuring the fault management server.

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 4: Monitoring and managing the IP Office system

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 41

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	✔	✔	✔	✔

Related topics:

Monitoring IP Office remotely using SSA on page 54
Monitoring IP Office remotely using SysMonitor on page 55
Configuring IP Office remotely using Web Manager on page 56
Configuring IP Office remotely using Manager on page 56
Configuring Server Edition systems remotely using IP Office Manager for Server Edition on page 57
Configuring Server Edition systems remotely using Web Control on page 59

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**.

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.

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 5: Monitoring the SSL VPN service

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 41.

Related topics:

Viewing the tunnel status on page 63
Monitoring alarms using SSA on page 67
Troubleshooting the SSL VPN service on page 68

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 64
Tunnel status field descriptions: detail table on page 65

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.

Value	Description
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.

Value	Description
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.
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 67

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

Name	Description
	• 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 • 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 69

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.

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

Chapter 6: Maintaining the SSL VPN service

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

Related topics:

Enabling and disabling the service on page 71
Resetting the password on page 77

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	✔	✔	✔	—
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 72
Disabling the service using Manager on page 73
Enabling the service using SSA on page 73
Disabling the service using SSA on page 74
Enabling the service using a short code on page 74
Disabling the service using a short code on page 75
Enabling and disabling the service using set-based administration on page 75
Enabling and disabling the service using programmable keys on page 76

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 34. 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 34. 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 77

Resetting the password using Manager on page 78

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 63.

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 63.

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.

Index