VPNremote for the 4600 Series IP Telephones

Release 2.1

Administrator Guide

19-600753
Issue 3
June 2007

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

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

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites and does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

http://www.avaya.com/support

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf). Be aware that there may 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 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 Web site:

http://www.avaya.com/support

Providing telecommunications security

Telecommunications security (of voice, data, and video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or person working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Use (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including, but not limited to, human and data privacy, intellectual property, material assets, financial resources, labor costs, and legal costs).

Your responsibility for your company's telecommunications security

The final responsibility for securing both this system and its networked equipment rests with you, an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources, including, but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products.

Trademarks

Avaya is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Avaya support

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

http://www.avaya.com/support

Contents

About this book

The guide provides network administrator and end-user configuration information for the Avaya VPNremote for the 4600 Series IP Telephones. This document is to be used in conjunction with the *Avaya 4600 Series IP Telephone LAN Administrator Guide*.

In the following pages, information is provided describing configuration of the Avaya VPNremote for the 4600 Series IP Telephones (VPNremote Phone) from the Administrator's perspective, including items that should be noted as part of installation. For more information regarding Administrator configuration, see Chapter 2: Configuration.

In addition, end-user configuration information is provided to assist the end user in installing and configuring the VPNremote Phone in their small office home office (SOHO) environment with minimal assistance from corporate IT or Telephony groups. For more information regarding end-user installation and configuration, see *VPNremote for 4600 Series IP Telephone User Installation and Configuration Quick Start*, document number 19-601608.

What products are covered

The following products is covered in this manual:

- Avaya VPNremote for the 4600 Series IP Telephones

  The Avaya 4600 Series IP Telephones that support the VPNremote Phone firmware includes the following devices:

  - Avaya 4610SW IP Telephone
  - Avaya 4620SW IP Telephone
  - Avaya 4621SW IP Telephone
  - Avaya 4622SW IP Telephone
  - Avaya 4625SW IP Telephone

Online Documentation

The online documentation for the Avaya VPNremote for the 4600 Series IP Telephones is located at the following URL:

http://www.avaya.com/support

Related Documentation

- Request For Comments (RFC)

  The following RFCs have been implemented: 2401, 2407, 2408, 2409, 3715, 3947, 3948, 2406, 2411.

  http://www.ietf.org/html.charters/OLD/ipsec-charter.html

The following documents are available on the Web site under Find Documentation and Downloads by Name:

- *Avaya VPNremote for the 4600 Series IP Telephones User Installation and Configuration Quick Start* (19-601608).

  This document provides instructions for the end user to install the VPNremote Phone in their SOHO. This document also provides information on how to enter their user name and password using the telephone keypad.

- *Avaya Administrator Guide for Communication Manager* (03-300509)

  This document provides an overall reference for planning, operating, and administering your Communication Manager solution.

- *Avaya 4600 IP Series Telephone, Release 2.4, LAN Administrator Guide* (555-233-207)

  This document provides a description of Voice over IP and describes how to administer the DHCP, TFTP, and HTTP servers. This guide also covers how to troubleshoot operational problems with the 4600 Series IP Telephones and the servers.

- Avaya 4600 Series IP Telephone, Release 2.2.1, Installation Guide (555-223-128)

  This document provides detailed information on how to install the 4600 Series IP Telephone product line and troubleshoot problems with the telephones.

- *Avaya VPNremote Client 4.1 Administrator Guide* (June 2002)

  This document provides a description of the VPNremote Client software and describes how to administer the software.

- *Avaya Security Gateway Configuration Guide for VPNos 4.6* (670-100-602)

  This document provides configuration and administration information for the Avaya SG5, SG5X, SG200, SG203, and SG208 Security Gateway that are upgraded to VPNos 4.6 and Avaya VSU devices that are upgraded to VPNos 3.X.

Chapter 1: Introduction

The Avaya VPNremote for 4600 Series IP Telephones (VPNremote Phone) is an Avaya H.323 IP Telephone with an integrated virtual private network (VPN) client and an advanced web-enabled graphical display.

VPNremote Phone overview

The VPNremote Phone provides enterprise telephony services at a remote or small office home office (SOHO) location through a secure VPN connection to the user's Enterprise Communication Manager infrastructure. The VPNremote Phone uses a high-speed connection to the Internet and then to the VPN solution in the enterprise network.

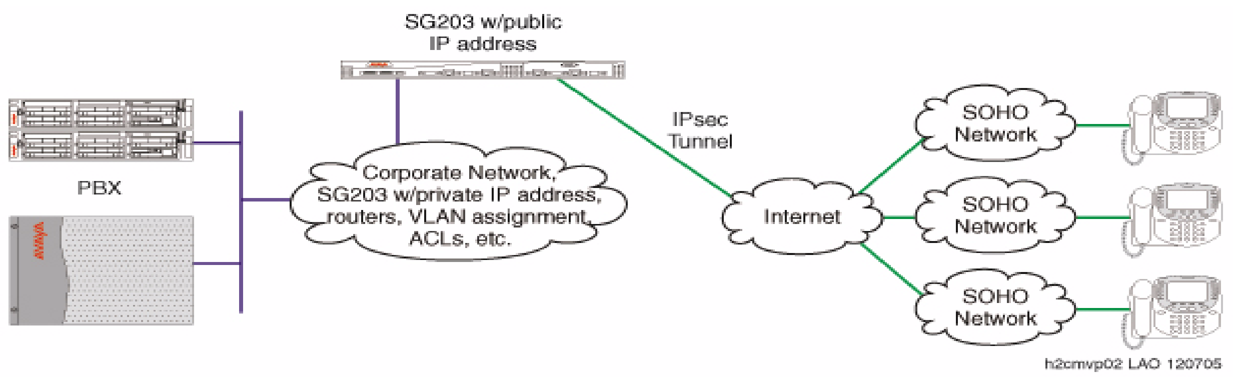
The Avaya VPNremote for 4600 Series IP Telephones provides a significant improvement on communications capabilities of SOHO users. The VPNremote Phone provides users with an extension on an enterprise PBX over a secure VPN connection in a single-box solution.

For additional information regarding the 4600 Series IP Telephones, see the *Avaya 4600 Series IP Telephone, Release 2.4, LAN Administrator Guide*.

Beginning with Release 2, the VPNremote Phone is capable of implementation in Enterprise networks with third-party devices. For more information regarding supported third-party devices, see VPNremote Phone features in Release 2.

The VPNremote Phone is targeted to work with most SOHO network configurations. Figure 1 illustrates a possible corporate network configuration with an Avaya SG203 at the headend device with three VPNremote Phones connected through secure VPN connections.

Figure 1: VPNphone in a corporate network with an Avaya SG203 as the headend device


SG203 w/public IP address
PBX
Corporate Network, SG203 w/private IP address, routers, VLAN assignment, ACLs, etc.
IPsec Tunnel
Internet
SOHO Network
SOHO Network
SOHO Network
h2cmvp02 LAO 120705

VPNremote Phone features in Release 2.1

The following summarizes a number of significant feature, performance, and usability enhancements provided by VPNremote Phone, Release 2.1.

- **Third-party devices**– Beginning in this release, the VPNremote Phone supports the following third-party devices:

Supported Device	Minimum Software Requirement
Checkpoint VPN	Any
Nortel Contivity VPN Appliances	V06_00.310 or higher

- **Self Installer**– Beginning in this release, the VPNremote Phone supports an administrator configured self installer that allows the end user to perform the configuration while located outside of the Enterprise network. The user can be located at a Small Office Home Office (SOHO) or at home. A small DHCP and TFTP server, the Self Installer, can be executed from a PC connected to the network port on the telephone.
- **Quality test (Qtest)**– The VPNremote Phone tests the connection quality.

VPNremote Phone features in Release 2

The following summarizes a number of significant feature, performance, and usability enhancements provided by VPNremote Phone, Release 2.

- **Third-party devices**– Beginning in this release, the VPNremote Phone supports the following third-party devices:

Supported Device	Minimum Software Requirement
Cisco VPN 3000 Series Concentrators	Any
Cisco PIX 500 Series Security Appliances	Any
Juniper Networks NetScreen series VPN devices	Screen OS 5.1.0 and higher

Supported Device	Minimum Software Requirement
Juniper Networks Secure Services Gateway 500 Series devices	Screen OS 5.1.0 and higher
Juniper Networks Integrated Security Gateway (ISG) Series devices	Screen OS 5.1.0 and higher

- **Automatic discovery of UDP encapsulation method**– The VPNremote Phone will automatically select the correct UDP encapsulation mode during the connection process.
- **SNMP and syslog support through the VPN tunnel**– The VPNremote Phone can be SNMP polled through the VPN tunnel, and syslog messages can be securely sent through the VPN tunnel.
- **Copy TOS**– Allows TOS to be copied to ESP header packets.
- **Selectable connectivity test**– The VPNremote Phone tests connectivity to the known hosts. This test can be set to first time, always, or never.

VPNremote Phone features in Release 1

The following summarizes a number of significant feature, performance, and usability enhancements provided by VPNremote Phone, Release 1.

- **H.323 IP Telephone** – The VPNremote Phone is a fully featured Avaya H.323 IP Telephone. The H.323 IP Telephone includes the following features:
  - A large display area that allows up to 12 application-specific buttons to be presented and labeled at one time.
  - Twelve line/feature buttons
  - Four softkeys
  - Fixed buttons that provide access to powerful capabilities such as: local telephone and call server-based features, speed dialing, a Call Log, and a Wireless Markup Language (WML) browser.
- **Integrated IPSec Client** – The VPNremote Phone contains an integrated IPSec VPN Client that supports the following IPSec protocols:
  - Internet Protocol Security (IPSec)

    VPNremote Phone supports IPSec. VPNremote Phone supports IPSec when implemented under an existing implementation of an IP protocol. For additional information regarding IPSec protocol support, see the *Avaya Security Gateway Configuration Guide for VPNos 4.6*.

- Internet Key Exchange (IKE)

  VPNremote Phone supports the standard IKE key management protocol for IPSec. For additional information regarding IKE protocol support, see the *Avaya Security Gateway Configuration Guide for VPNos 4.6.*

- Internet Security Association and Key Management (ISAKMP)

  VPNremote Phone supports the standard IISAKMP protocol for IPSec. For additional information regarding IS AK MP protocol support, see the *Avaya Security Gateway Configuration Guide for VPNos 4.6.*

Chapter 2: Configuration

This section provides administrators with information on how to configure the Avaya VPNremote for 4600 Series IP Telephone as a VPNremote Phone.

The enterprise network must be configured with a security device. Corporate firewalls and routers must be configured to allow IPSec tunnels from VPNremote Phone to the security device. The VPNremote Phone is compatible with the Avaya Security Gateway and with third-party security devices using IKE Extended Authentication (Xauth) with Preshared Key. For the list of supported third-party devices, see VPNremote Phone features in Release 2 and VPNremote Phone features in Release 2.1. For a list of supported third-party devices and their configurable system parameters, see Table 4, System parameters on the VPNremote Phone.

Beginning with VPNremote Phone, Release 2.1 there are two methods of configuration for the VPNremote Phone: Pre-deployment configuration and Self Installer configuration. Although both methods require Administrator configuration, the pre-deployment is completed in the Enterprise network environment with the most current software installed prior to deployment to end user. In the Self Installer configuration, the software installation and configuration is started by the Administrator by preconfiguring the Self Installer file, but is completed by the end user by executing the Self Installer file in their Small Office Home Office (SOHO) or home environment.

Configuration preparation

To insure that the end user is able to configure VPNremote Phone in their SOHO environment and to connect to the enterprise network, you can preconfigure the IP telephone prior to deployment to the end user or preconfigure the self installer for the end user.

To preconfigure the IP telephone prior to deployment to the end user, follow the recommended preconfiguration method starting at Step1. To preconfigure the self installer for the end user, follow the recommended preconfiguration method starting at Step 3.

The prior to deployment configuration is to be completed while the IP telephone is connected to the enterprise network. By using this method, the administrator maximizes their configuration time; and minimizes end user configuration requirements that are entered using the telephone keypad. This preconfiguration method also protects the end user’s login ID and password.

The self installer configuration file is completed by the administrator. The self installer file includes the VPNremote Phone software and all the specific configuration settings that are unique to the enterprise. The administrator configure the self installer file, creates a.zip file that includes the self installer and any documentation, and places the.zip file on a network drive that is accessible by the end user.

Preconfiguration Method

Following is the recommended preconfiguration method, including the sequence and procedures:

1. Allow access into and out of the corporate firewall through VPN tunnels. For Avaya Security Gateways, see The VPNremote Phone and the Avaya Security Gateway. For third-party security devices, see Configuring the VPNremote Phone for third-party devices.
2. Convert the 4600 Series IP Telephone. See Converting an IP Telephone to VPN IP Telephone.
3. Collect application file and source file information. See Collecting the VPNremote Phone source file information.
4. Create the VPN setting file (46vpnsetting.txt). See Modifying the VPNremote Phone VPN settings file.
5. Download the VPN firmware from the TFTP server. See Downloading the VPN firmware.
6. Configure the VPN settings to meet the configuration parameters for each VPNremote Phone site, see Configuring the VPN Settings.
7. Create and administer a new extension with Communication Manager, Release 2.3 or higher. For additional information see Preparing Communication Manager for the VPNremote Phone.
8. Install and test the IP telephone on the enterprise network. For additional information, see the *Avaya 4600 Series IP Telephone Installation Guide*.
9. Ship preconfigured device to the end user.

Preparing the security device for the VPNremote Phone

Beginning with Release 2.0, the VPNremote Phone is capable of implementation in Enterprise networks with Avaya Security Gateway devices and with third-party security devices. Whichever security device is implemented in the network, it must be configured to create a VPN tunnel with the VPNremote Phone. To configure the Avaya security gateway to communicate with the VPNremote Phone, see The VPNremote Phone and the Avaya Security Gateway. To configure third-party security devices to communicate with the VPNremote Phone, see The VPNremote Phone and the third-party device.

Tip:

Refer to the security device documentation for the procedures to configure a specific device.

Once the security device is configured to allow VPN tunnels, verify the VPN configuration by using the device manufacturer provided IPSec client to create a VPN tunnel. Upon establishing a VPN tunnel, you have verified that the security device is configured correctly. Communication between the VPNremote Phone and the security device should be successful.

The VPNremote Phone and the Avaya Security Gateway

The VPNremote Phone user authentication configuration uses the Avaya proprietary client configuration download (CCD) protocol to establish a transport layer security (TSL) session with the security gateway. This authentication process is called the handshake. During the handshake, the VPNremote Phone verifies that the certificate presented by the security gateway is issued by a trusted Avaya Certificate Authority (CA).

Once the VPNremote Phone and security gateway have established device authentication, the VPNremote Phone user credentials are sent to the security gateway. If the security gateway can verify the VPNremote Phone user credentials, the security gateway sends the necessary information to establish an IPSec security association (SA). This information includes the following:

- IP address from the Client IP Address Pool

  The client IP address pool is a range of IP addresses configured on the Avaya security gateway specifically for IPSec clients. The VPNremote Phone uses an IP address from the client IP address pool when communicating with the network on the private side of the security gateway.

- IP address of the FQDN Server

  The FQDN server is located on the private side of the security gateway. The security gateway is capable of delivering IP addresses from the FQDN server to the VPNremote Phone.

  Tip:

  Verify that the security gateway is configured to deliver FQDN server IP addresses to the IPSec clients.

  The VPNremote Phone ignores default domain prefixes sent by the security gateway. Verify that the security gateway is configured to send fully qualified domain names only.

- List of protected subnets

  The list of protected subnets can be specified by the security gateway. This list can be accessed by the IPSec clients.

  Tip:

  Avaya recommends that all zeros be configured as the subnets that are accessible by the IPSec clients.

- Welcome banner

  The welcome banner in the Avaya security gateway is known as the Client Legal Message and is normally used to provide security related information to end users of the VPN. The welcome banner can also be used to deliver configuration information to the phone by using structured commands. When used for configuration, user information in the message is displayed on the phone display.

Tip:

Use this configuration delivery method when the configuration parameters or to update configuration parameters are the same for all VPNremote Phones.

The user authentication allows VPN traffic to flow through the corporate firewalls to the security gateway, which, in turn, allows the VPNremote Phone to communicate with the Enterprise Communication Manager infrastructure.

Configuring the VPNremote Phone for the Avaya Security Gateway

VPNremote Phone users who login to the VPN through the Avaya security gateway must have their user authentication configured on that security gateway.

As a minimum, a user name and the password for each remote user must be configured on the security gateway. User names can be up to 128 characters long and can contain any character except a comma (,). Note that once you add a user name, you cannot change the name.

For additional information regarding configuring the security gateway for the VPNremote Phone, see the *Avaya Security Gateway Configuration Guide for VPNos 4.6*.

Table 1 lists the configurable system parameters for the Avaya Security Gateway. For more information regarding system parameters, see Appendix C: System Parameters Customization.

Table 1: System parameters on the VPNremote Phone

Supported Device	System Parameter Values

Avaya Security Gateway	Set the following values:
	With local authentication:
	`NVVPNCFGPROF(1)`
	With Secure ID:
	`NVVPNCFGPROF(1)`
	`NVVPNPSWDTYPE(3)`
	`NVVPNAUTHTYPE(2)`
	With RADIUS:
	`NVVPNCFGPROF(1)`
	`NVVPNAUTHTYPE(2)`

For more information regarding customizing VPNremote Phone system parameters, see Appendix C: System Parameters Customization.

The VPNremote Phone and the third-party device

The VPNremote Phone is compatible with third-party security devices using IKE Extended Authentication (Xauth) with Preshared Key. Xauth performs user authentication on the third-party device in a separate authentication phase after the IKE authentication phase 1 is complete. The VPNremote Phone uses the Preshared Key to authenticate the security device.

Table 2 lists the IKE authentication phase 1 proposal list that VPNremote Phone sends during IKE phase 1 negotiation. Verify that the security device accepts one of the following IKE parameters:

Table 2: IKE Phase 1 parameters

Parameter	Parameter
AES-128, HMAC-SHA1, DH-2	DES, HMAC-MD-5, DH-2
AES-128, HMAC-MD5, DH-2	AES-192, HMAC-SHA1, DH-2
3DES, HMAC-SHA1, DH-2	AES-192, HMAC-MD-5, DH-2
3DES, HMAC-MD-5, DH-2	AES-256, HMAC-SHA1, DH-2
DES, HMAC-SHA1, DH-2	AES-256, HMAC MD5, DH-2

Table 3 lists the IKE authentication phase 2 proposal list that VPNremote Phone sends during IKE phase 2 negotiation. Verify that the security device accepts one of the following IKE parameters:

Table 3: IKE Phase 2 parameters

Parameter	Parameter
ESP, AES-128, HMAC-SHA1, DH-None	ESP, DES, HMAC-MD-5, DH-None
ESP, AES-128, HMAC-MD-5, DH-None	ESP, AES-192, HMAC-SHA1, DH-None
ESP, 3DES, HMAC-SHA1, DH-None	ESP, AES-192, HMAC-MD-5, DH-None
ESP, 3DES HMAC-MD-5, DH-None	ESP, AES-256, HMAC-SHA1, DH-None
ESP, DES, HMAC-SHA1, DH-None	ESP, AES-256, HMAC-MD-5, DH-None

Once the VPNremote Phone and security device have established device authentication, a temporary secure path is created allowing the VPNremote Phone to send user credentials are sent to the security device. If the security device can verify the VPNremote Phone user credentials, the security device sends the necessary information to establish an IPSec connection. This information includes the following:

- IP address from the Client IP Address Pool

  The client IP address pool is a range of IP addresses configured on the Avaya security gateway specifically for IPSec clients. The VPNremote Phone uses an IP address from the client IP address pool when communicating with the network on the private side of the security gateway.

- IP address of the FQDN Server

  The FQDN server is located on the private side of the security device. The security device is capable of delivering IP addresses from the FQDN server to the VPNremote Phone.

  Tip:

  Verify that the security gateway is configured to deliver FQDN server IP addresses to the IPSec clients.

  The VPNremote Phone ignores default domain prefixes sent by the security device. Verify that the security device is configured to send fully qualified domain names only.

- Welcome banner

  The welcome banner in the Avaya security gateway is known as the Client Legal Message and is used to deliver configuration information to the VPNremote Phone during the VPN creation.

  Tip:

  Use this configuration delivery method when the configuration parameters or to update configuration parameters are the same for all VPNremote Phones.

  Currently, the only third-party device that supports the use of the Welcome Banner are the Cisco VPN 3000 Series Concentrators.

The user authentication allows VPN traffic to flow through the corporate firewalls to the security gateway, which, in turn, allows the VPNremote Phone to communicate with the Enterprise infrastructure.

Configuring the VPNremote Phone for third-party devices

Table 4 lists the configurable system parameters for the supported devices. For more information regarding system parameters, see the 46vpnsetting_readme.txt file.

Table 4: System parameters on the VPNremote Phone

Supported Device	System Parameter Values

Cisco VPN 3000 Series Concentrators	Set the following values:
	`NVVPNCFGPROF(3)`
	`NVVPNSVENDOR(2)`
	`NVVPNAUTHTYPE(4)`
	`NVIKEXCHGMODE(1)`
	`NVIKEIDTYPE(11)`
	`NVIKECONFIGMODE(1)`

Cisco PIX 500 Series Security Appliances	Set the following values:
	`NVVPNCFGPROF(3)`
	`NVVPNSVENDOR(2)`
	`NVVPNAUTHTYPE(4)`
	`NVIKEXCHGMODE(1)`
	`NVIKEIDTYPE(11)`
	`NVIKECONFIGMODE(1)`

Juniper Networks NetScreen series VPN devices	Set the following values:
	`NVVPNCFGPROF(5)`
	`NVVPNSVENDOR(1)`
	`NVVPNAUTHTYPE(4)`
	`NVIKEIDTYPE(3)`
	`NVIKEXCHGMODE(1)`
	`NVIKECONFIGMODE(1)`

Juniper Networks Secure Services Gateway 500 Series devices	Set the following values:
	`NVVPNCFGPROF(5)`
	`NVVPNSVENDOR(1)`
	`NVVPNAUTHTYPE(4)`
	`NVIKEIDTYPE(3)`
	`NVIKEXCHGMODE(1)`
	`NVIKECONFIGMODE(1)`

Juniper Networks Integrated Security Gateway (ISG) Series devices	Set the following values:
	`NVVPNCFGPROF(5)`
	`NVVPNSVENDOR(1)`
	`NVVPNAUTHTYPE(4)`
	`NVIKEIDTYPE(3)`
	`NVIKEXCHGMODE(1)`
	`NVIKECONFIGMODE(1)`

Checkpoint VPN	Set the following values:
	`NVVPNCFGPROF(2)`
	`NVVPNAUTHTYPE(3)`

	1 of 2

Table 4: System parameters on the VPNremote Phone (continued)

Supported Device	System Parameter Values

Nortel Contivity VPN Appliance	Set the following values:
	With Password:
	`NVVPNCFGPROF(11)`
	`NORTELAUTH(1)`
	With SecureID:
	`NVVPNCFGPROF(11)`
	`NVVPNPSWDTYPE(3)`
	`NORTELAUTH(3)`
	With RADIUS:
	`NVVPNCFGPROF(11)`
	`NORTELAUTH(2)`

Any Security Device (Generic) with Preshared Key (PSK)	Set the following values:
	`NVVPNCFGPROF(6)`
	`NVVPNSVENDOR(4)`
	`NVVPNAUTHTYPE(3)`
	`NVIKECONFIGMODE(2)`
	`NVIKEXCHGMODE(1)`
	`NVIKEIDTYPE(3)`

Any Security Device (Generic) with IKE Extended Authentication (Xauth)	Set the following values:
	`NVVPNCFGPROF(7)`
	`NVVPNSVENDOR(4)`
	`NVVPNAUTHTYPE(4)`
	`NVIKEIDTYPE(3)`
	`NVIKEXCHGMODE(1)`
	`NVIKECONFIGMODE(1)`

	2 of 2

For more information regarding customizing VPNremote Phone system parameters, see Appendix C: System Parameters Customization.

Converting an IP Telephone to VPN IP Telephone

Use the following procedure and the telephone key pad to convert a non-VPNremote IP telephone into a VPNremote telephone:

1. Allow the telephone to initialize and register with Communication Manager.
2. After the phone is registered, set the GROUP for each phone you want to upgrade to a VPN IP telephone to 876. To initiate the GROUP command from the telephone key pad, press:

   `Mute 4-7-6-8-7 #`
3. After the GROUP command is initiated, enter **`8-7-6 #`** (V-P-N #) for the New value. Use Page LEFT key to erase any errors.
4. Press # to save the new value.

   `Save new value?`

   `* = no #=yes`

Collecting the VPNremote Phone source file information

In order to modify the VPNremote Phone source files, you must collect the following information:

- Security device manufacturer

  The manufacturer of the security device: Avaya, Nortel, Cisco, Checkpoint, or Nokia
- IP address or FQDN name of the primary security device

  The IP address of the Avaya security gateway is 172.145.21.110. The domain name of the Avaya security gateway is west1.avaya.com. The IP address of the
- IP address or FQDN name of the back-up security device
- IP address or FQDN name of the file server for the VPNremote Phones

  The TFTP server where the VPNremote Phone downloads the firmware.
- Group name (IKE ID) for third-party security devices

  The group name and group password for third-party devices.

In addition to the previous list, you may want to collect the following optional information:

- IKE phase 1 Diffie-Hellman group

  The telephone and the security device use IKE phase 1 to create a secure path to exchange encryption keys.

- IKE phase 2 Diffie-Hellman group

  The telephone and security device use IKE phase 2 to create a subsequent key when the Perfect Forward Security (PFS) option is used.
- IP address of FQDN name of the SMNP management station

  The IP address or FQDN of the SNMP management system that will be receiving status messages from the VPNremote Phone.
- SNMP read string

  The character string that the SNMP management station presents to identify themselves to each other.
- IP address or FQDN name of the syslog server

  The server that receives the syslog message from the VPNremote Phone.
- IP address or FQDN name of the call server

  The Communication Management system that controls the VPNremote Phone.
- Default domain prefix

  The prefix for the FQDN. For example,.com,.net, or.biz.

Modifying the VPNremote Phone VPN settings file

After you have downloaded and installed the VPNremote Phone firmware, you must modify the VPN settings file for the end user.

To modify the VPN settings file:

1. Unzip the VPNremote Phone firmware to a temporary location. The firmware includes the following files:
   - 46XXvpn.scr
   - 46vpnupgrade.scr
   - 46vpnsetting_template.txt
   - Application files for all supported 4600 series IP telephones
2. Use the information collected in Collecting the VPNremote Phone source file information to modify the VPN setting parameters in the 46vpnsetting.txt file. See Table 5 for the list of VPN settings to be modified.

Table 5: VPN source file and VPN setting parameters

Source File Information	VPN Setting Parameter
IP address or FQDN name of the primary security device	NVSGIP
IP address or FQDN name of the back-up security device	NVBACKUPSGIP
IP address or FQDN name of the file server for the VPNremote Phones	NVVPNFILESRVR
Group name (IKE ID) for third-party security devices	NVIKEID
IKE phase 1 Diffie-Hellman group	NVPFSDHGRP
IKE phase 2 Diffie-Hellman group	SNMPADD
IP address of FQDN name of the SMNP management station	SNMPSTRING
SNMP read string	LOGSRVR
IP address or FQDN name of the syslog server	MCIPADD
IP address or FQDN name of the call server	DOMAIN

3. Save the VPN settings file as **`46vpnsetting_template.txt`**.
4. Add the following lines to the beginning of the new 46upgrade.scr file:

```
IF $GROUP SEQ 876 goto DEFVPN
GOTO NOVPN
# DEFVPN
GET 46xxvpn.scr
goto END
# NOVPN
```

5. Save the 46upgrade.scr file.

6. Copy all VPNremote Phone firmware files and any related installation documentation to the.zip file.
7. Copy the.zip file on a user accessible down-load server.
8. Notify the user of the location of the down-load server.

Downloading the VPN firmware

Prior to configuring the VPNremote Phone, you must first install the VPNremote Phone firmware on an existing internal TFTP server. Install the VPNremote Phone firmware files on the same TFTP server that the existing IP telephones 2.3 firmware or higher.

Note:

The TFTP server should not be accessible from outside the enterprise network without a VPN connection.

To download the firmware:

1. Verify that the file server is configured to upgrade the telephone firmware.
2. Copy the VPNremote Phone software files to the TFTP server. The VPNremote Phone firmware files must be on the same TFTP server as the existing IP telephones firmware.

Configuring the VPN Settings

Once the firmware has successfully downloaded to the IP Telephone, you are now ready to configure the VPN settings. The 46vpnsettings_template.txt and the 46vpnsetting_readme.txt files are populated with the settings that are used by the VPNremote Phone to create the VPN tunnels. It is recommended that the administrator edit the VPN settings files to set the configuration parameters for VPNremote Phone users.

Note:

For a detailed list of VPN settings, see the 46vpnsetting_readme.txt file.

At startup, the phone will attempt to establish a VPN connection using the configured VPN parameters. The user is given the option to change the VPN parameters. To change the VPN parameters, the user can press the Edit button indicated on the VPN startup screen. The Edit button gives the user a screen that can be used to change the VPN parameters.

If the phone is up and registered with Communication Manager, the user may also edit the VPN parameters by entering the VPNMOD command as detailed below.

Use the following procedure and the telephone key pad to configure or edit the VPN Settings:

1. To initiate the VPNMOD command from the telephone key pad, press:

   `Mute V-P-N-M-O-D #` or **`Mute 8-7-6-6-6-3 #`**

   `VPN Start Mode: BOOT`

   `* = Modify # = OK`

2. Press **`*`** to modify your VPN settings.
3. Select the VPN option to change by using the gray buttons on the left of the display. Press the **Server** button, or the first gray button, to change the VPN server IP address.
4. Enter the IP address of the SOHO network. Press the **Done** button at the lower left corner of the display to return to the configuration options. The IP address of the SOHO network must be provided by the end user.
5. Select the VPN option to change by using the gray buttons on the left of the display. Press the **User Name** button, or second gray button, to change the VPN user name.

   The user name is the same name used to login to the enterprise network using remote client software.

6. Enter the user name using the telephone key pad. Press the alpha-numeric keys until the desired letter appears. Use the Case button, or fifth gray button, to switch between upper-case letters and lower-case letters. Use the left and right arrow keys at the bottom of the display to move left or right in the user name. Press the **Done** button at the lower left corner of the display to return to the configuration options.
7. Select the VPN option to change by using the gray buttons on the left of the display. Press the **Password** button, or third gray button, to change the VPN password.

   The password is the same password used to login to the enterprise network using VPNremote Client.

8. Enter the password using the telephone key pad. Press the alpha-numeric keys until the desired letter appears. Use the Case button, or fifth gray button, to switch between upper-case letters and lower-case letters. Use the left and right arrow keys at the bottom of the display to move left or right in the user name. Press the **Done** button at the lower left corner of the display to return to the configuration options.
9. Select the VPN option to change by using the gray buttons on the left of the display. Press the **Authentication mode** button, or forth gray button, to change the authentication mode.
10. Select the VPN option to change by using the gray buttons on the left of the display. Press the **Password Type** button, or fifth gray button, to change the password type.
11. Press the fifth button on the right side of the display to scroll through the password type options.
12. Select the VPN option to change by using the gray buttons on the left of the display. Press the **VPN Start Mode** button, or sixth gray button, to change the VPN start mode.

13. Press the sixth button on the right side of the display to scroll through the VPN start mode options. Select **Boot** and press **#**.
14. Press the right arrow key to move to the next display.
15. Select the VPN option to change by using the gray buttons on the left of the display. Press the **Encapsulation** button, or the first gray button, to change the encapsulation option.
16. Press the first button on the right side of the display to scroll through the encapsulation options. Select **Disable** and press **#**.
17. The Syslog Server option is not configured.
18. Press **Done** to complete the configuration.

Preparing Communication Manager for the VPNremote Phone

A VPNremote Phone is configured the same as other IP telephones on the Avaya Media Server running Avaya Communication Manager. Even though the VPNremote Phone is physically located outside of the corporate network, the VPNremote Phone will behave the same as other Avaya IP telephones located on the LAN once the VPN tunnel has been established.

VPNremote Phone as a single extension on Communication Manager

The VPNremote Phone user can have a single extension on the Avaya Media Server running Avaya Communication Manager. A single extension allows the user to be connected to the Communication Manager from one location at a time - either the office or the SOHO.

If the desired configuration is to connect to Communication Manager from both the office and the SOHO, you must configure VPNremote Phone as a separate extension that has a bridged appearance of the office extension. For more information on a bridged appearance on Communication Manager, see VPNremote Phone as a bridged appearance on Communication Manager.

For additional information regarding Communication Manager configuration, see the *Administrator Guide for Avaya Communication Manager*.

VPNremote Phone as a bridged appearance on Communication Manager

The VPNremote Phone user can have a bridged appearance of the office extension on the Avaya Media Server running Avaya Communication Manager. A bridged appearance allows the user to be connected to the Communication Manager from two locations at the same time. As a call comes in, both telephones ring. If a voicemail message is received and the message indicator light is configured, the light appears on both telephones.

Tip:

When going into the office, remember to minimize the ringer volume on the SOHO extension.

The bridged appearance configuration is the most common configuration for VPNremote Phone users.

For additional information regarding Communication Manager configuration, see the *Administrator Guide for Avaya Communication Manager*.

Installing the VPNremote Phone in the enterprise network

The Avaya VPNremote for 4600 Series IP Telephone is a standard Avaya 4600 Series IP Telephone with an additional VPNremote Client capability. The installation of the VPNremote Phone in the enterprise network is the same as the installation of any Avaya 4600 Series IP Telephones.

For detailed instructions on how to install the VPNremote Phone into the enterprise network, see the *Avaya 4600 Series IP Telephone Installation Guide*.

Deploying the VPNremote Phone

Deploy the VPNremote Phone to the end user. When the end user installs the VPNremote Phone in their home network, the telephone will initialize and display a user ID and password error. The end user must enter their user name and password that they use to login to their enterprise network using remote client software.

Appendix A: Avaya VPNremote for 4600 Series IP Telephones Installation Checklist

The checklist on the following page is provided for your convenience for supplying your users with essential installation information.

Table 6: VPNremote Phone Installation Checklist

Item	Value	Description
VPNremote Phone IP Address	The default value is 0.0.0.0 when using DHCP.	In the SOHO network uses DHCP, set this value to 0.0.0.0 # (default value). Otherwise, enter the IP address used by the VPNremote Phone in the SOHO network.
Call Server Port Address	The default value is 1719 unless otherwise stated by your administrator.	This IP address is the IP address of the CLAN inside the enterprise.
Gateway IP Address	If DHCP is being used, press # to accept the default values. Otherwise end user will confirm address.	This IP address is the IP address of the SOHO router.
Network Mask	If DHCP is being used, press # to accept the default values. Otherwise end user will confirm address.	This IP address is the network mask for SOHO network.
TFTP File Server		This IP address is the TFTP file server inside the enterprise that contains the configuration and update files.
Extension of your VPNremote Phone		Depending on the telephony configuration, this extension may or may not be the same extension as your office telephone. Check with you telephony administrator to confirm your extension.
		1 of 2

Table 6: VPNremote Phone Installation Checklist (continued)

Item	Value	Description
VPNremote Phone password		Depending on the telephony configuration, this password may or may not be the same password as your office telephone. Check with you telephony administrator to confirm your password.
VPN server		This is the public IP address of the security gateway.
VPN user name		End user will enter.
VPN password		End user will enter.
		2 of 2

Appendix B: Troubleshooting

This chapter describes problems that might occur during installation and configuration of the Avaya VPNremote for 4600 Series IP Telephones and possible ways of resolving these problems.

This chapter contains the following sections:

- Descriptions of error conditions and methods for resolving them.
- Error and status messages, and methods for resolving them.
- Syslog

Error Conditions

The following information describes some of the most common issues that may be seen and how to trouble shoot them.

Authentication Failures

- Check User ID and password configured on phone
- Check Event log on Security gateway
- Check Configured User ID and password on Gateway
- If external authentication is used such as Radius, check connectivity between SG and Radius and Radius User configuration

TCP/IP Connection Failure

- Confirm VPN server address is correct.
- Confirm the Gateway is available
- Confirm VPNPhone has internet connectivity
- Confirm TCP port 1443 is not blocked by any external device between phone and the security gateway.

  The SOHO router may be configured to allow only outgoing TCP connection on port 80 for HTTP and port 443 for HTTPS. There may also be a firewall in front of security gateway that may not be configured to allow an incoming TCP connection on port 1443.

SSL Connection Failure

- Confirm security device is accepting SSL connections

  This requires access to the device’s Web interface or SSH access.

General Phone Errors and Behaviors

- Contact DHCP/TFTP administrator, L2Q parms in option 43/176 or xxx.SCR script file.

  The VPNremote Phone is experiencing a looping condition. This condition is caused by the gateway IP address being set to 0.0.0.0. Change the device IP address to the static security device IP address or DHCP.

- Loading ……. is not seen during startup and mute light flashes.

  Check the bootcode version. Older version such as 1.9x is not compatible with the latest software version.

IKE and IPSec Negotiation Failures

- Enable IKE Logging on the security device
- Perform TCP dumps from the security device console/SSH connection.

Phone fails to register

- Confirm the VPN tunnel was built

  1. Check if the security associations (SA) are built on security device under Monitor/VPN from the Web interface.
  2. When the VPN Phone starts, does it access the TFTP server through the VPN tunnel. If it does then the tunnel is up to that network. Check to see if the call server is on the same subnet as the TFTP server. If configured IP group in SG covers both address, then access should be available.

- Perform a TCP dump on interfaces of the central security device. Check to see if the esp packets are arriving from the phone during the time it should be registering.

  1. If not Check the L3 Audio and Signaling values. If set to 46/34, change to zero and restart phone and check tcpdump.
  2. If TOS bits are being copied to esp packet on the security device side, Communication Manager configuration may need to be changed. The above may be require when ISPs block TOS marked packets.

Error and Status Messages

The 4600 Series IP Telephones issue messages in English only. The IP telephones also display messages from the switch, which can issue messages in the local language outside the United States.

Note:

The following error messages are for the VPNremote Phone only. For additional information on the 4600 Series IP Telephone error messages, see the 4600 Series IP Telephone, Release 2.2.1, Installation Guide.

Most of the messages in following tables display only for about 30 seconds, and then the telephone resets.

Table 7 describes the list of all error messages that pertain to the VPN tunnel setup failures that the VPNremote Phone might display.

Table 7: VPN Tunnel Setup Failures

Error Message	Avaya Profile	Third-Party Profile	Possible Cause	Possible Solution
TCP Connection timed out.	Yes	N/A	Security gateway not accessible or unresponsive to TCP connection.	Verify end-user login ID and password, and that the network is up.
SSL Handshake failed	Yes	N/A	SSL 1443 connection failed.	Verify end-user login ID and password.
Invalid server certificate	Yes	N/A	Security device certificate issue.	Verify that the security device certificate is valid.
Unknown certificate issuer	Yes	N/A	SSL handshake during VPN setup failed because the server certificate provided by the gateway is not signed by the appropriate.	Verify that the VPNremote Phone is connecting to an Avaya device.
				1 of 4

Table 7: VPN Tunnel Setup Failures (continued)

Error Message	Avaya Profile	Third-Party Profile	Possible Cause	Possible Solution
Server authentication mechanism failing	Yes	N/A	An externally configured authentication source (Radius Server) and Security Gateway cannot communicate.	Verify communication with external authentication source.
IKE Phase 1 no response	Yes	Yes	Security device is busy. For all Profiles: Security device cannot be reached because the firewall is blocking incoming UDP packets on port 500. This is on the security device side or home router is blocking outgoing UDP packets on port 500.	For all Profiles: Verify that the firewall accepts UDP packets on port 500. Verify that the security device allows outgoing UDP packets on port 500.
			For third-party profile: Group Name (IKE ID) is incorrect. IKE ID type is incorrect. Phase 1 proposal mismatch.	For third-party profiles: Verify group name. Verify IKE IK type. Verify phase 1 proposal.
				2 of 4

Table 7: VPN Tunnel Setup Failures (continued)

Error Message	Avaya Profile	Third-Party Profile	Possible Cause	Possible Solution
IKE Phase 2 no response.	No	Yes	Security device is busy. IKE phase 2 proposal is mismatched. Vendor-specific features are enabled. List of protected IP groups do not match.	Verify IKE proposal is correct, disable vendor-specific features, and/or verify protected IP groups.
Failed to reach known host.	Yes	N/A	VPNphone was unable to reach known host such as the TFTP server or call server address.	Verify that the TFTP server address is correct. Verify that the call server address is correct.
IKE Preshared key (PSK) mismatch.	No	Yes	PKS (Group password) is incorrect.	Verify that the IKE PSK is correct.
				3 of 4

Table 7: VPN Tunnel Setup Failures (continued)

Error Message	Avaya Profile	Third-Party Profile	Possible Cause	Possible Solution
DNS needed for resolving security device name.	Yes	Yes	The system could not resolve the security device fully qualified domain name (FQDN). DNS query sent to resolve security device FQDN failed or has timed out.	Check the DNS server connection. Verify that the FQDN is correct.
Security device name resolution failed.	Yes	Yes	The system could not resolve the security device fully qualified domain name (FQDN). DNS query sent to resolve security device FQDN failed or has timed out.	Check the DNS server connection. Verify that the FQDN is correct.
				4 of 4

Table 8 describes the list of all error messages that pertain to the VPN tunnel setup failures that the VPNremote Phone might display.

Table 8: Authentication Errors

Error Message	Possible Cause
Authentication failure, User Blocked	User is blocked for “x” minutes from “x” number of incorrect logins.
Invalid password OR user name	Incorrect user name or password entered.
Phone brand rejected by SG	Incorrect phone brand configured on gateway.
VPN Topology not supported	Multiple central site devices configured which is not a supported configuration.
Empty Gate Keeper	No call server addresses configured.

Note:

All error messages will provide the option to display more information or edit the configuration.

Syslog

Adding the IP address of the SYSLOG server will enable Sysloging of VPN module. This SYSLOG server is meant to catch log messages while tunnel setup is in progress hence the syslog server must be accessible without the tunnel.

Appendix C: System Parameters Customization

Use the 46vpnsetting_readme.txt file located in the VPNremote Phone firmware folder to customize the system parameters.

For additional definitions and information on how to change IP telephone parameters, see the *Avaya 4600 Series IP Telephone, Release 2.3, LAN Administrator Guide*, *Server Administration* chapter, *Administering Options for the 4600 Series IP Telephones*.

For additional information on the Script File, see the *Avaya 4600 Series IP Telephone, Release 2.3, LAN Administrator Guide*, *Server Administration* chapter, *Contents of the Upgrade Script* section. We recommend that you administer options on the 4600 Series IP Telephones using script files.

Appendix D: Firewall Rules

The VPNremote Phone is capable of communicating with the Avaya security gateway through the firewalls of the small office home office (SOHO) gateway and the security gateway. Use Table 9 to create the SOHO firewall rules. For information on the Avaya security gateway firewall rules, see the *Avaya Security Gateway Configuration Guide for VPNos Release 4.6*, 670-100-602.

Table 9: VPNremote Phone SOHO firewall rules

Source	Source Range	Configurable Source	Protocol	Destination	Dest. Range	Configurable Dest.	Response from Dest.
Phone	Any	No	TCP TLS	SG public interface	1443	No	Yes
Phone	2070	No	UDP IKE/IPsec	SG public interface	500	No	Yes
Phone	2070	No	UDP IKE/IPsec	SG public interface	4500	No	Yes
Phone	500	No	UDP IKE/IPsec	SG public interface	500	No	Yes
Phone	4500	No	UDP IKE/IPsec	SG public interface	4500	No	Yes
SD public interface	N/A	N/A	ESP (51)	Phone	N/A	N/A	N/A
Phone	N/A	N/A	ESP (51)	SG public interface	N/A	N/A	N/A

Index