VPN Setup Guide
for 9600 Series IP Telephones
Release 3.1

16-602968
Issue 1
November 2009

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.

For full legal page information, please see the complete document, Avaya Legal Page for Hardware Documentation, Document number 03-600759.

To locate this document on our Web site, simply go to http://www.avaya.com/support and search for the document number in the search box.

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 referenced elsewhere within this documentation, and Avaya 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

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

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

http://www.avaya.com/support

Software License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

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 Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s):

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.

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 identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's Web site at:

http://support.avaya.com/ThirdPartyLicense/

Interference

Using a cell, mobile, or GSM telephone, or a two-way radio in close proximity to an Avaya IP Telephone might cause interference.

Contents

Chapter 1: Introduction

About This Guide

This guide provides information describing VPN configuration, use, and troubleshooting from both the Administrator's and end user's perspective, including items that should be noted as part of installation. For more information regarding administrative configuration, see Chapter 2: VPN Overview.

End-user configuration information is provided to assist the end user in installing and configuring a 9600 Series IP Telephone in their small office home office (SOHO) environment with minimal assistance from corporate IT or Telephony groups. Procedures for end user viewing and updating VPN settings are also provided.

Use this setup guide in conjunction with the standard setup instructions in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide* (Document Number 16-300698).

Note:

Unlike all other 9600 Series IP Telephones, the 9610 IP Telephone is not VPN-capable and cannot be used as part of your VPN.

Intended Audience

This guide provides network administrator and end-user information for a Virtual Private Network (VPN) for 9600 Series IP Telephones. If you are an administrator, use this document in conjunction with the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide* (Document Number 16-300698).

CAUTION:

Avaya does not provide product support for many of the products mentioned in this document, including security gateways, remote Internet access devices such as DSL or cable modems, file servers, DNS servers, or DHCP servers. Take care to ensure that there is adequate technical support available for these products and that they are properly configured, otherwise the IP telephones might not be able to operate correctly.

Document Organization

The guide contains the following sections:

Chapter 1: Introduction	Provides an overview of this guide.
Chapter 2: VPN Overview	Provides an overview of the supported VPN functionality and identifies differences from the 4600 Series IP Telephones' implementation of VPN.
Chapter 3: Configuring the VPN	Describes the equipment and resources required to properly configure the 9600 Series IP Telephones for VPN functionality.
Chapter 4: Viewing VPN Settings	For users with view-only privileges, describes how to access and view VPN Settings using the Avaya (A) Menu.
Chapter 5: Changing VPN Settings	For advanced users with update privileges, describes how to access, add, or update VPN settings using the VPN Special Procedure and the Local Administrative (Craft) Procedures Menu.
Chapter 6: User Authentication and VPN Sleep Mode	Describes how to enter and update the VPN user name and password. Also covers how to deactivate the VPN tunnel and put the phone into sleep mode.
Chapter 7: VPN Troubleshooting Guidelines	Provides a list of errors that might occur during VPN startup and operation, and suggested resolutions.
Appendix A: VPN Parameters	Summarizes the parameters potentially used as part of VPN administration and functionality for 9600 Series IP Telephone users.
Appendix B: Glossary of Terms	Provides a glossary of terms used in this document or which are generally applicable to 9600 Series IP Telephones.

Change History

Issue 1	This is the first release of this document, issued in November 2009 as part of Software Release 3.1.

Online Documentation

See the Avaya support site at http://www.avaya.com/support for 9600 Series IP Telephone technical and end user documentation.

Related Documentation

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

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

- *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide* (Document Number 16-300698)

  This document provides a detailed description of how to administer the 9600 Series IP Telephones for use in your Enterprise environment, including VPN administration.

- *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-300694)

  This document provides a detailed description of how to install and maintain the 9600 Series IP Telephones for use in your environment.

Customer Support

For 9600 Series IP Telephone support, call the Avaya support number provided to you by your Avaya representative or Avaya reseller.

Information about Avaya products can be obtained at the following URL:

http://www.avaya.com/support

Chapter 2: VPN Overview

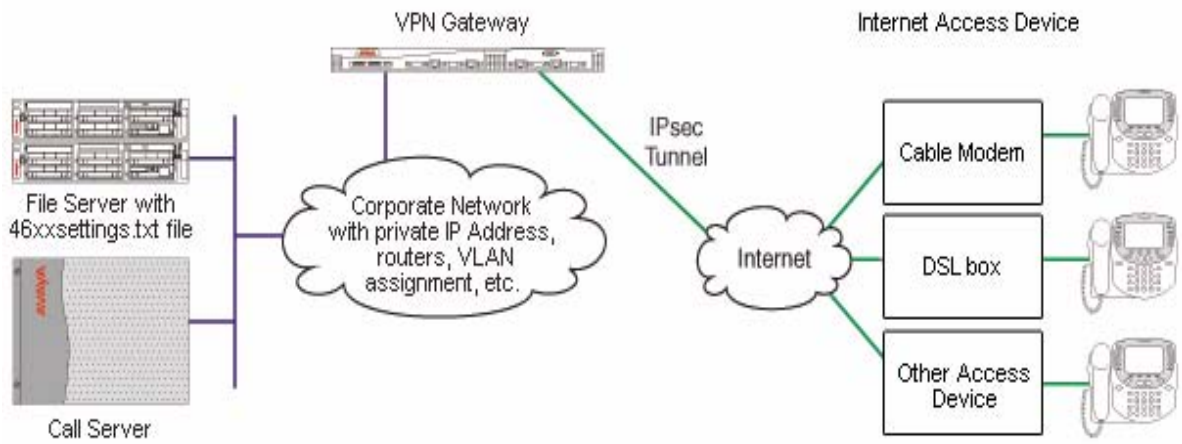
Introduction

Setting up a virtual private network provides enterprise telephony services for remote or small office home office (SOHO) locations through a secure VPN connection to the user's Enterprise Communication Manager infrastructure. A VPN uses a high-speed connection to the Internet and then to the VPN-administered solution in the enterprise network. VPNs provide a significant improvement of the communications capabilities of SOHO users.

9600 Series IP Telephone Release 3.1 provides the capability to implement a VPN in Enterprise networks with third-party devices. For more information regarding third-party devices, see Supported Third-Party Security Gateways.

Figure 1 illustrates a possible corporate network configuration with three 9600 Series IP Telephones connected through secure VPN connections.

Figure 1: VPN Configuration



Differences Between 4600 Series and 9600 Series IP Telephone VPNs

Review this section if you already have a VPN in place for 4600 Series IP Telephones. There are several differences between the structure and administration for each type of telephone series, namely:

- A 9600 Series VPN telephone is administered by setting the applicable system parameters using the ***46xxsettings.txt*** file. This is the same settings file you already use for the non-VPN system parameters you currently customize for both 9600 Series and 4600 Series IP Telephones. A 4600 Series VPN uses a unique settings file (46vpnsetting.txt) to administer applicable system parameters instead of the 46xxsettings.txt file.
- 9600 Series IP VPN Telephones do not support the Avaya SG203 security gateway, whereas 4600 Series IP VPN Telephones do.
- 9600 Series IP Telephone VPNs use an enhanced security process:
  - End users have a separate access code and permission settings that allow access only to VPN settings rather than general access to all local administrative (Craft) procedures.
  - VPN users are assigned a unique VPN password which can be administered to be erased on VPN termination or telephone reset; this measure prevents unauthorized users from automatically re-establishing a VPN tunnel.
  - Users with valid VPN credentials can be prevented from using each other's telephones by setting the NVVPNUSERTYPE parameter to allow the VPN user name to be changed only through the settings file or the VPN Settings Craft procedure.
- 9600 Series IP Telephone VPNs provide longer DNS names, up to 255 characters whereas 4600 Series VPNs limit DNS names to 16 characters.
- 9600 Series IP VPN Telephones do not support user entry of an SCEP challenge password.
- 9600 Series IP Telephones do not support the NVSECSGIP and NVBACKUPSGIP parameters. See Appendix A: VPN Parameters for a detailed list of the VPN system parameters applicable to a 9600 Series IP Telephone.

Supported Third-Party Security Gateways

Beginning with software Release 3.1, third-party devices by the following vendors are supported:

- Checkpoint
- Cisco

- Juniper
- Nokia
- Nortel

Avaya does not guarantee compatibility with all security gateway devices or software provided by a particular vendor, nor is every possible configuration of such devices supported. In general, Release 3.1 supports the following capabilities:

- Release 3.1 contains an integrated IPSec VPN Client that supports these IPSec protocols:
  - Internet Protocol Security (IPSec),
  - Internet Key Exchange (IKE), and
  - Internet Security Association and Key Management (ISAKMP).
- Pre-Shared Key (PSK) with or without XAUTH,
- RSA (Rivest-Shamir-Adleman) signatures with or without XAUTH,
- NAT traversal, and
- SCEP.

Chapter 3: Configuring the VPN

Introduction

This section outlines configuration requirements and setup options, and provides administrators with information on how to configure 9600 Series IP Telephones for a VPN.

Preliminary Configuration Requirements

The enterprise network must be configured with a security gateway. Corporate firewalls and routers must be configured to allow IPSec tunnels from the remote phone(s) to the security gateway. For the list of supported third-party devices, see Supported Third-Party Security Gateways on page 10. For a list of configuration system parameters, see Appendix A: VPN Parameters.

Technicians or administrators can stage phones centrally and pass an administered phone to an end user, or use the standard settings file. In the latter case, place VPN parameters in the beginning of the 46xxsettings.txt file before model-specific settings. The possible VPN configuration methods are:

- Centralized administration of some or all VPN functionality by trained technicians/ administrators, using either the settings file and/or the local (Craft) procedure for VPNs. The administered telephone is then passed to the user.
- Remote administration of VPN functionality by users who are either trained in, or who have been provided specific documentation to guide them in the administration process, generally involving the VPN Special Procedure.

Avaya recommends that administrators perform these preliminary configuration steps:

- Load the 9600 Series IP Telephone with the latest (R3.1 or greater) software,
- Configure the phone to connect to the Enterprise infrastructure, and
- Provide the end users with information for VPN access from their small office home office (SOHO) environment.

Important:
Never "downgrade" a telephone on your VPN to a software release prior to R3.1, as VPN operation will either fail or not operate properly.

Configuration Preparation

To ensure that the end user is able to configure a 9600 Series IP Telephone in their SOHO environment and to connect to the enterprise network, administrators can pre-configure the IP telephone prior to deployment to allow the remote 9600 Series IP Telephone to establish a connection over the VPN tunnel and if applicable, to provide authentication parameter values.

The administrator completes the initial configuration while the IP telephone is connected to the enterprise network and prior to deployment to the end user. When more than five or six phones require configuration, Avaya recommends the administrator use the settings file for configuring the VPN telephones, with the exception of the User Name and User Password.

Following is the recommended pre configuration method, including the sequence and procedures:

1. Allow access into and out of the corporate firewall through VPN tunnels, see Preparing the Security Gateway.
2. Configure the VPN parameters to meet the configuration parameters for each remote site, see Configuring VPN System Parameters.
3. If necessary, create and administer a new extension on Communication Manager, Release 5.1 or higher. For additional information see Preparing Avaya Communication Manager.
4. Install and test the IP telephone on the enterprise network. For additional information, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-600394).
5. Send the pre configured telephone to the end user with specific instructions for VPN remote setup.

Preparing the Security Gateway

Install the security gateway in accordance with the vendor's instructions.

Authentication credentials must be configured to allow users to establish a VPN connection.

At a minimum, you must configure a user name and password for each remote user. User names can be up to 16 characters long and can contain any character except a comma (,).

Configuring the VPN Settings

The administrator can populate the 46xxsettings.txt file with all or some of the settings that are used to create the VPN tunnels and for authentication, depending on whether or not end users will be given permission to add/change settings.

Note:

For a detailed list of VPN settings in the 46xxsettings.txt file, see Appendix A: VPN Parameters.

At startup, the phone will attempt to establish a VPN connection using the configured VPN parameters. Users with permission to do so can view, add, or change the VPN parameters.

Simple Enrollment Certificate Protocol (SCEP)

The 9600 Series IP Telephones support Media Encryption (SRTP) and use built-in Avaya certificates for trust management. Trust management involves downloading certificates for additional trusted Certificate Authorities (CA) and the policy management of those CAs. Identity management is handled by Simple Certificate Enrollment Protocol (SCEP) with phone certificates and private keys. SCEP can apply to your VPN operation or to standard enterprise network operation. SCEP is described in the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide* (Document Number 16-300698), however for ease of VPN setup, the applicable parameters are also included this guide, in Appendix A: VPN Parameters. A few pointers regarding SCEP follow:

- If the SCEP server is outside of the corporate firewall, telephones connecting to the corporate network over a VPN connection can be configured to establish the SCEP connection using an HTTP proxy server to reach the SCEP server. In this instance, use the WMLPROXY system parameter to configure the HTTP proxy server.
- When SCEP is initiated the telephone will attempt to contact an SCEP server via HTTP, using the value of the configuration parameter MYCERTURL as the URI.
- SCEP supports the use of an HTTP proxy server.
- The telephone creates a private/public key pair, where each key has a length equal to the value of the configuration parameter MYCERTKEYLEN. The public key and the values of the configuration parameters MYCERTCAID, MYCERTCN, MYCERTDN and SCEPPASSWORD are used in the certificate request.

Configuring VPN System Parameters

Appendix A: VPN Parameters lists the system parameters that you need to configure for VPN tunnel establishment, and in general. Certain parameters will be set automatically based on the VPN security gateway you indicate in the NVVPNCFGPROF parameter in the 46xxsettings.txt file or using the Special VPN procedure; see VPN Configuration Profiles in Appendix A: VPN Parameters for information on these automatically-set configuration parameters.

Important:

When using the settings file to establish VPN values, place all of your VPN parameters before any model-specific parameters.

For detailed information regarding system parameters, see Appendix A: VPN Parameters.

Administrative Pre-Requisites for Authentication

Authentication is performed during VPN tunnel initialization only if the NVXAUTH parameter is set to "enabled." The following system parameters are used for authentication and are described in detail in Appendix A: VPN Parameters:

- NVXAUTH - Specifies whether XAUTH user authentication is enabled or disabled; must be enabled for authentication.
- NVVPNUSER - Specifies the user name to use during VPN authentication; can be null and entered on the VPN User Name Entry screen.
- NVVPNPSWD - Specifies the user's VPN password; can initially be null and entered on the VPN Password Entry screen if NVVPNUSER contains a non-null value and NVVPNUSERTYPE is set to "1" (user can edit the user name).
- NVVPNPSWDTYPE - Specifies whether the VPN user password will be stored, and if so, how it is stored.
- NVVPNUSERTYPE - Specifies whether the end user can ("1") or cannot ("2") change the VPN user name.

When authentication is enabled, three potential authentication entry screens display, depending on the values of these VPN authentication parameters. See User Authentication in Chapter 6: User Authentication and VPN Sleep Mode for a description of each authentication screen.

Preparing Avaya Communication Manager

A 9600 Series IP Telephone that will be used in your virtual private network is configured the same as other IP telephones on the call server running Avaya Communication Manager. Even though the phone is physically located outside of the corporate network, it will behave the same as other LAN-based Avaya IP telephones once the VPN tunnel has been established.

Note:

The end user can have either a single extension or a bridged extension on the 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. To connect to Communication Manager from both the office and the SOHO, configure the telephone as a separate extension that has a bridged appearance of the office extension.

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

Installing the 9600 Series IP Telephone

Installation of 9600 Series IP Telephones to be used in a VPN network is the same as for any Avaya 9600 Series IP Telephone. For detailed installation instructions, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide* (Document Number 16-600394).

If you are staging the telephones centrally before deploying them to the users, install and test the IP telephone on the enterprise network.

Important:
Telephones will attempt to establish a VPN connection only if the system parameter NVVPNMODE is set to "1" (Enabled). You can choose to permit your end users to change this value if a remote telephone will also be used within the enterprise environment.

Deploying the VPN-Ready 9600 Series IP Telephone

Deploy the telephone to the end user. When the end user installs the phone in the home network, what displays is dependent on the authentication policy you have set up and on the permission you have assigned to VPN users in the VPNPROC parameter. Typically, users of a centrally-staged telephone will see a screen requesting the VPN User Name and/or Password; once the VPN tunnel is established, the user experience is essentially the same as for a non-VPN phone:

- If you have set the VPNPROC parameter to "1" or "2" the Avaya Menu (or, for 9670G phones, the Home Screen) your VPN users see has a VPN Settings option. Users can either view (if VPNPROC = 1) or change (if VPNPROC=2) VPN settings.
- If you have set the VPNPROC parameter to "0" the VPN Settings option does not display as an Avaya Menu (or Home screen) option. Your users cannot view or change VPN settings.

Communicate the VPN Access Code (VPNCODE) to those users you have assigned permission to view or change VPN settings. While not recommended for security reasons, you can set VPNCODE to null (" ") to allow anyone you have given permission to view or change settings via VPNPROC to bypass access code entry when they want to view or update VPN settings.

Also provide each user with the appropriate chapter(s) in this guide describing how to access VPN Settings screen(s) as follows:

- Chapter 4: Viewing VPN Settings for those users you are permitting view-only access.
- Chapter 5: Changing VPN Settings for those users you are permitting to change VPN settings. Although these users can use the procedures in Chapter 5 to view settings as

well, you may also want to provide them with Chapter 4: Viewing VPN Settings to allow them to view the VPN Summary screen instead of the individual filtered screens.

- Chapter 6: User Authentication and VPN Sleep Mode if you have established authentication parameters, as covered in Administrative Pre-Requisites for Authentication.

Chapter 4: Viewing VPN Settings

Introduction

This chapter describes how to view the settings for your VPN. It contains procedures for accessing the VPN Settings Summary screen and provides descriptions for your settings.

Two methods are available to view VPN settings:

- Using the VPN Settings screen, available through the Avaya (A) Menu for all but the 9670G IP Telephone, and available through the Home Screen for the 9670.Typically, users without authorization to change settings use this screen to view VPN settings.
- Using the VPN Configuration screen, available through the VPN Settings Craft (local administrative) procedure. This screen is also used to change settings and requires special authorization; therefore, viewing settings using the VPN Configuration screen is described in Chapter 5: Changing VPN Settings. Your administrator must authorize your ability to *change* VPN settings. This includes providing you with a VPN Access Code and applicable procedures describing how to change the settings. If you have the proper authorization to change VPN settings, see Chapter 5: Changing VPN Settings for information.

Note:

As a security feature, the first time you use your remote phone over the Virtual Private Network or following a telephone reset or reboot, you may be asked to identify yourself so that you can be verified as a valid user and your user credentials can be validated. Chapter 6: User Authentication and VPN Sleep Mode explains the authentication process.

Note:

All 9600 Series IP Telephones except the 9670G require you to press a button/softkey to take an action like exiting a screen. On 9670G IP Telephones, all actions are touch-based and are taken or confirmed by touching a softkey on the screen.

Access Using the Avaya (A) Menu

Use this procedure If your administrator has instructed you to use the Avaya (A) Menu to access VPN settings and has provided you with a VPN Access Code.

Note:

If your VPN administration requires authentication of your user name and password, follow the steps in Chapter 6: User Authentication and VPN Sleep Mode before proceeding.

1. For all 9600 Series IP Telephones except the 9670, press the **Avaya (A) Menu** button. For a 9670G phone, touch **Home**.
2. For 9600 Series IP Telephones without administered WML applications, select **VPN Settings**.

   For 9600 Series IP Telephones with administered WML applications, select **Phone Settings** first, then **VPN Settings**.

   For the 9670, touch **Settings**, then **VPN Settings**.
3. If the phone prompts you to "Enter Password and press Enter (or OK)" use the dialpad to enter the VPN Access Code assigned by the administrator and press **Enter** or **OK**. On a 9670, enter the VPN Access Code and touch **Enter**. When the access code is validated the VPN Settings screen displays. See Viewing the VPN Settings Screen for a description of this screen.

Viewing the VPN Settings Screen

The VPN Settings screen is accessed through the Avaya (A) Menu (or the Home screen for the 9670), as described in Access Using the Avaya (A) Menu.

What you see on the VPN Settings screen depends on the type of security gateway used to connect your telephone to the corporate network and how your Virtual Private Network (VPN) was administered. For example, the settings information is "filtered" to show settings applicable to your specific VPN environment.

If more than one screen is required to display all the data relevant to your VPN, a right-facing navigation arrow displays at the top of the screen. Press (or if you have a 9670G IP Telephone, touch) that arrow to see additional settings; use the left-facing navigation arrow that displays to move backward from screen to screen.

Note:

If you are unfamiliar with a term used in the description, see Appendix B: Glossary of Terms. The "Associated System Parameter" column in the VPN Settings screen description below refers to the system parameters the administrator has set for your Virtual Private Network.

VPN Settings Screen

Line/Field	Description	Associated System Parameter
VPN	If "1" the Virtual Private Network is enabled. If "0" VPN is disabled.	NVVPNMODE
VPN Vendor	Name of the security gateway vendor.	NVVPNSVENDOR
Gateway Address	IP address of the VPN security gateway. This value allows the telephone to access the VPN tunnel.	NVSGIP
External Phone IP Address	External ("outer") IP address of the telephone in VPN mode.	NVEXTIPADD
External Router	External ("outer") router IP address in VPN mode.	EXTGIPADD or NVEXTGIPADD
External Subnet Mask	External ("outer") subnet mask in VPN mode.	NVEXTSUBNETMASK
External DNS Server	External ("outer") DNS server IP address in VPN mode.	EXTDNSSRVR or NVEXTDNSSRVR
Encapsulation	The port numbers used for IKE and IPsec UDP encapsulation, and support for NAT traversal.	NVVPNENCAPS
Copy TOS	Indicates whether to copy the TOS bits from the tunneled (inner) IP header to the tunnel (outer) IP header.	NVVPNCOPYTOS
		1 of 5

VPN Settings Screen (continued)

Line/Field	Description	Associated System Parameter
Auth Type	User authentication method for non-Nortel gateways: 3 = Pre-Shared Key (PSK) 4 = PSK with XAUTH 5 = RSA signatures with XAUTH 6 = Hybrid XAUTH 7 = RSA Signatures User authentication method for Nortel gateways: 1= Local credentials 2 = RADIUS credentials 3 = RADIUS SecurID 4 = RADIUS Axent	NORTELAUTH (for Nortel gateways only), otherwise NVVPNAUTHTYPE
VPN User Type	End user permission to change the VPN username: 1 = User can change the user name 2 = User cannot change the user name	NVVPNUSERTYPE
VPN User	The user name used for authentication.	NVVPNUSER
Password Type	Indicates if the VPN user password will be stored and how: 1 = Password can be alphanumeric and is stored in reprogrammable non-volatile memory as the NVVPNPSWD value. 2 = Password can be alphanumeric and is stored in volatile memory but will be cleared when the phone resets. 3 = Password can be numeric only and is stored in volatile memory that is cleared immediately after first-time password use. 4 = Password can be alphanumeric and is stored in volatile memory that is cleared immediately after first-time password use. 5 = Password can be alphanumeric and is stored in volatile memory that is cleared when the user invokes VPN Sleep Mode and when the telephone resets.	NVVPNPSWDTYPE

2 of 5

VPN Settings Screen (continued)

Line/Field	Description	Associated System Parameter
User Password	If a user password exists, it is shown here as 8 asterisks (********)	Blank if user password has no value (null), otherwise 8 asterisks
IKE ID (Group Name)	This field and the next three fields display only if your VPN meets the conditions for displaying IKE PSK.	NVIKEID
Pre-Shared Key (PSK)	Pre-Shared Key.	Blank if PSK has no value (null), otherwise 8 asterisks.
IKE ID type	This field and the next five fields display only if your VPN meets the conditions for displaying IKE Phase 1. Values are: 1 = ID_IPV4_ADDR 2 = ID_FQDN 3 = ID_USER_FQDN 9 = ID_DER_ASN1_DN 11 = ID_KEY_ID	NVIKEIDTYPE
IKE Xchg Mode	1 = Aggressive Mode 2 = Main Mode Identity Protection	NVIKEXCHGMODE
IKE DH Group	1 = First Oakley Group 2 = Second Oakley Group 5 = 1536-bit MODP Group 14 = 2048-bit MODP Group 15 = 3072-bit MODP Group	NVIKEDHGRP
IKE Encryption Alg	Algorithm 0 = Any 1 = AES-CBC-128 2 = 3DES-CBC 3 = DES-CBC 4 = AES-CBC-192 5 = AES-CBC-256	NVIKEP1ENCALG
IKE Auth. Alg	Authentication algorithm for IKE: 0 = Any 1 = MD5 2 = SHA	NVIKEP1AUTHALG
		3 of 5

VPN Settings Screen (continued)

Line/Field	Description	Associated System Parameter
IKE Config Mode	1 = Use the ISAKMP configuration method for setting certain applicable values. 2 = This setting is turned off (disabled) because a generic PSK profile is in effect.	NVIKECONFIGMODE
IPsec PFS DH Group	This field and the next four fields display only if your VPN meets the conditions for displaying IKE Phase 2. This field specifies the Diffie-Hellman Group to be used for establishing the IPsec SA (also known as PFS). If this value is not "0", a new Diffie-Hellman exchange will be initiated for each IKE Phase 2 Quick Mode exchange, where the proposed DH group will be as specified by the value of NVPFSDHGRP, and the meaning of the values will be the same as those specified above for NVIKEDHGRP.	NVPFSDHGRP
IPsec Encryption Alg	The encryption algorithm to propose for use during IKE Phase 2 negotiation. Values are: 0 = Any 1 = AES-CBC-128 2 = 3DES-CBC 3 = DES-CBC 4 = AES-CBC-192 5 = AES-CBC-256 6 = Null	NVIKEP2ENCALG
IPsec Auth. Alg	The authentication algorithm to propose for use during IKE Phase 2 negotiation. Values are: 0 = Any 1 = MD5 2 = SHA	NVIKEP2AUTHALG

4 of 5

VPN Settings Screen (continued)

Line/Field	Description	Associated System Parameter
Protected Network	Specifies the IP address range that will use the VPN tunnel.	If a list, the (first) value of NVIPSECSUBNET
IKE over TCP	This field displays only if your VPN meets the conditions for displaying IKE Over TCP. Specifies whether and when to use TCP as a transport protocol for IKE: Never = Never use TCP as a transport protocol for IKE. Auto = Use IKE over UDP first, and if that isn't valid use IKE over TCP. Always = Always use TCP as the transport protocol for IKE.	NVIKEOVERTCP
		5 of 5

For detailed information regarding system parameters, see Appendix A: VPN Parameters.

Chapter 5: Changing VPN Settings

Introduction

This chapter describes how to change VPN parameter settings. Prior to performing any of the procedures in this section, and based on whether the telephones will be set up centrally or remotely, the administrator should establish appropriate values for VPN tunnel connection and user authentication. Applicable VPN system parameters are listed in Appendix A: VPN Parameters.

Three methods are available to *change* VPN settings:

- Invoking the VPN Special Procedure from the local administrative (Craft) procedure menu using the same access method as you would for any local procedure. This method requires that the person accessing the local procedure knows the local procedure access password set in the PROCPSWD parameter.
- Invoking the VPN Special Procedure using the VPN Access Code, when administrative permission to change settings has been granted by setting the VPNPROC parameter to "2."
- Invoking the VPN Settings option from the Avaya (A) Menu (or the Home screen for a 9670) using the VPN Access Code (if VPNPROC is set to "2").

Note:

All 9600 Series IP Telephones except the 9670G require you to select a line or desired action and press a button/softkey to act upon your selection. On 9670G IP Telephones, all actions are touch-based; for example, text/numeric entry uses an on-screen keyboard, and actions are taken or confirmed by touching the applicable line, feature, icon, or softkey on the screen. The procedures that follow apply to non-9670G phones and should be adjusted accordingly for the 9670's touch screen.

VPN Settings Screens (VPN Special Procedure)

If you are not familiar with the applicable values for a specific parameter setting, see Appendix A: VPN Parameters.

Accessing VPN settings

Only the administrator or those end users with administrative permission to view or change VPN settings (via the VPNPROC parameter setting of "2") can access VPN Special Procedure, which contains a series of filtered VPN Settings screens. You also need a VPN Access Code or a Local Administrative (Craft) Procedure access code to access the settings this chapter describes.

Note:

As a security feature, the first time you use your remote phone over the Virtual Private Network or following a telephone reset or reboot, you may be asked to identify yourself so that you can be verified as a valid user and your user credentials can be validated. Chapter 6: User Authentication and VPN Sleep Mode explains the authentication process.

Access using the Avaya (A) Menu:

Use this procedure If your administrator has instructed you to use the Avaya (A) Menu to access VPN settings and has provided you with a VPN Access Code.

1. For all 9600 Series IP Telephones except the 9670, press the **Avaya (A) Menu** button. For a 9670G phone, touch **Home**.
2. For 9600 Series IP Telephones without administered WML applications, select **VPN Settings**.

   For 9600 Series IP Telephones with administered WML applications, select **Phone Settings** first, then **VPN Settings**.

   For the 9670, touch **Settings**, then **VPN Settings**.
3. If the phone prompts you to "Enter Access Code and press Enter (or OK)" use the dialpad to enter the VPN Access Code assigned by the administrator and press **Enter** or **OK**. On a 9670, enter the VPN Access Code and touch **Enter**. When the access code is validated:

   The VPN Configuration screen displays. See Viewing or changing settings using the VPN Special Procedure on page 30 for information on updating the settings.

Access using the VPN Special Procedure

Use this procedure if your administrator has instructed you to use the VPN Special Procedure to update VPN settings. The VPN Special Procedure is a series of filtered screens showing settings applicable to your specific VPN setup.

1. At any time following telephone login, press **Mute**.
2. Enter the VPN Access Code provided by your administrator.
3. Press #.

4. Proceed to Viewing or changing settings using the VPN Special Procedure on page 30.

Access using the Local Administrative (Craft) Procedure Menu

Use this procedure if your administrator has instructed you to use the Craft (local administrative) procedure to update VPN settings. This access method allows you to access the VPN Special Procedure, to change VPN settings.

During Telephone Startup:

1. During startup, invoke local procedures by pressing ***** to display the Craft Access Code Entry screen:

```
Enter code:__
#=OK
```

2. Enter the local dialpad procedure password (0 to 7 numeric digits), as specified by the system administrator in the system value PROCPSWD. For security purposes, the telephone displays an asterisk for each numeric dialpad press. If you are using a 9670G IP Telephone, and need to backspace during password entry, use the Contacts button; for other 9600 Series phones, use the left arrow button or the designated softkey.
3. Press # when password entry is complete.

   The entry is compared to the PROCPSWD value. If they match, the telephone displays the Craft Local Procedure screen, "Select procedure and press Start."
4. For all 9600 Series IP Telephones except the 9670G, use the navigation arrows to scroll to and highlight **VPN**, then press **Start** or **OK**. Or scroll to **VPN** and press the corresponding line button. For the 9670G IP Telephone, scroll to **VPN** if it not already displayed; touch the line on which **VPN** appears.

During Normal Telephone Operation:

1. Invoke the local procedures (Craft) menu by pressing the **Mute** button, entering the local (dialpad) procedure password (0 to 7 numeric digits), then pressing the # button. If you are using a 9670G IP Telephone and need to backspace during password entry, use the Contacts button; for other 9600 Series phones, use the left arrow button or the designated softkey

   A 6-second timeout is in effect between button presses after pressing the **Mute** button. If you do not press a valid button within 6 seconds of pressing the previous button, the collected digits are discarded. In this case, no administrative option is invoked.

   The entry is compared to the PROCPSWD value. If they match, the telephone displays the Craft Local Procedure screen, and prompts "Select procedure and press Start."
2. For 9600 Series IP Telephones except the 9670G, use the navigation arrows to scroll to and highlight **VPN**, then press **Start** or **OK**. Or scroll to **VPN** and press the corresponding line

button. For the 9670G IP Telephone, scroll to **VPN** if it is not already displayed; touch the **VPN** line.

3. Proceed to Viewing or changing settings using the VPN Special Procedure.

Viewing or changing settings using the VPN Special Procedure

Access the VPN Special Procedure, a filtered series of configuration screens, through the local administrative (Craft) Procedures menu, as described in Access using the VPN Special Procedure or Access using the Local Administrative (Craft) Procedure Menu. To change VPN settings you must have:

- administrative permission to access the local administrative procedure menu (set administratively using the system parameter PROCSTAT), and
- an administrative procedure password (set administratively using the system parameter PROCPSWD), and
- permission to update VPN settings (set administratively using the system parameter VPNPROC of "2" to Update), and
- you must know the VPN Access Code (set administratively using the system parameter VPNCODE).

What you see on the VPN Configuration screens depends on the type of security gateway used to connect the telephone to the corporate network and how your Virtual Private Network (VPN) is administered. For example, settings information is "filtered" to show settings applicable to your specific VPN environment. Like a PC-style "wizard" settings display on a series of screens, the display of which is dependent on the actions you take on the current screen.

Navigating configuration screens and changing data

More than one screen is required to display all the data relevant to your VPN. In this case, the **Right** and **Left** navigation arrows move forward and back through the screen sequence applicable to your VPN. Pressing (or touching, for the 9670) the **Right Arrow** after updating one or more values on a screen saves the updated information and brings up the next applicable screen.

Important:
All changes are effective and saved when you press/touch the **Right Arrow** to navigate to the next screen. Navigating **Left** after making any change to one or more fields/lines on a particular screen *discards* those changes does not save any information you might have entered on that screen.

Select the field you want to change by positioning the cursor and pressing **Change**, or for a 9670, by touching the line you want to change. In general, when you press/touch **Change** the current value toggles to the next higher data value. For example, if the Gateway Vendor line shows "Nortel" (the fifth and last Gateway Vendor currently supported) and you select that line

and press/touch the Change softkey, the Gateway Vendor name changes to "Juniper/Net Screen" (the first Gateway Vendor supported). If the Gateway Vendor line shows "Juniper/Net Screen" (the first Gateway Vendor supported) and you select that line and press/touch the Change softkey, the Gateway Vendor name changes to "Cisco" (the second Gateway Vendor supported), and so on.

Changes you make to any one screen might cause a different screen to be shown next. For example, pressing **Change** on line/field names shown with an ellipsis (...) causes the VPN Text Entry screen to display to allow you to enter text. When you indicate you want to change a line containing an IP Address, the IP Address screen displays to allow that type of entry. After entering text or an IP address, press **Save** to post your entry and return to the previous screen where you can then press the **Right Arrow** to save your change(s) and display the next applicable settings screen.

After changing one or more fields/lines on the current screen, press the **Right Arrow** to save any changes you made and move to the next screen.

General VPN Settings - General screen

The General VPN Settings screen is the first screen displayed when you access the VPN Special Procedure or the VPN option on the Local Administrative (Craft) Procedures Menu. This screen provides basic information about your virtual private network.

Line/Field	Description	Associated System Parameter
VPN	Indicates whether the Virtual Private Network is enabled or disabled.	NVVPNMODE
VPN Vendor	Name of the security gateway vendor for your VPN.	NVVPNSVENDOR
Gateway Address...	IP address of the VPN security gateway. This value allows the telephone to access the VPN tunnel.	NVSGIP
External Phone IP Address...	External ("outer") IP address of the telephone in VPN mode.	NVEXTIPADD
External Router...	External ("outer") router IP address in VPN mode.	EXTGIPADD or NVEXTGIPADD
External Subnet Mask...	External ("outer") subnet mask in VPN mode.	NVEXTSUBNETMASK
	1 of 2	

Line/Field	Description	Associated System Parameter
External DNS Server...	External ("outer") DNS server IP address in VPN mode.	EXTDNSSRVR or NVEXTDNSSRVR
Encapsulation	The port numbers used for IKE and IPsec UDP encapsulation, and support for NAT traversal.	NVVPNENCAPS
Copy TOS	Indicates whether to copy the TOS bits from the tunneled (inner) IP header to the tunnel (outer) IP header.	NVVPNCOPYTOS
		2 of 2

In most cases, the next screen displayed is the Generic Authentication Type screen. If your security gateway VPN Vendor is Nortel, a Nortel Authentication Type screen displays instead:

Generic Authentication Type screen

This screen shows the type of authentication used by your VPN (based on the system parameter NVVPNAUTHTYPE). When you press/touch **Change** the authentication type changes to the next-higher value. Values in the order in which they appear as you press **Change** are:

If the Authentication Type Code (NVVPNAUTHTYPE) is:	This description displays:
3	PSK
4	PSK with XAUTH
5	RSA signatures with XAUTH
6	Hybrid XAUTH
7	RSA signatures

When the Authorization Type is PSK with XAUTH, RSA signatures with XAUTH, or Hybrid XAUTH, the next screen displayed is the User Credentials screen. If the Authorization Type is PSK, the next screen displayed is the IKE PSK screen. If the Authorization Type is RSA signatures, the next screen displayed is the IKE Phase 1 screen. You must press/touch the **Right Arrow** to save any change you made and to display the next screen.

Nortel Authentication Type screen

If your VPN uses a Nortel security gateway, this screen shows the type of authentication it uses (based on the system parameters NVVPNSVENDOR (value = 5) and NORTELAUTH). When you press/touch **Change** the authentication type changes to the next-higher value. Values in the order in which they appear as you press **Change** are:

If the Authentication Type Code (NORTELAUTH) is:	This description displays:
1	Local credentials
2	RADIUS credentials
3	RADUIS SecurID
4	RADIUS Axent

After viewing or changing the value, press/touch the **Right Arrow** to save any change you made and to display the User Credentials screen.

User Credentials screen

This screen displays three lines of user-specific information.

Line/Field	Description	Associated System Parameter
VPN User Type	End user permission to change the VPN username: If the user can change the user name, the description "Any" displays here. If the user cannot change the user name, the description "1 User" displays here and no change can be made to this line.	NVVPNUSERTYPE
	1 of 2	

Line/Field	Description	Associated System Parameter
VPN User...	The user name used for authentication. Pressing the **Change** softkey on this line brings up the VPN Text Entry screen so that (if permitted) you can enter a new user name.	NVVPNUSER
Password Type	The description indicates if the VPN user password will be stored and how. For example, when the NVVPNPSWDTYPE value is "3" the description "Numeric OTP" displays to indicate the VPN Password can be numeric only and is stored in volatile memory that is cleared immediately after first-time password use. Use the **Change** softkey to move from one description to another. If your password is stored in memory (as indicated by a description of either "Save in flash" or "Erase on reset") the next screen displayed is the User Password Entry screen. If your password type is other than the above descriptions and the type of authentication (NVVPNAUTHTYPE) is RSA Signatures with XAUTH or Hybrid XAUTH, the IKE Phase 1 screen displays instead. If none of those passwords types is applicable, the IKE PSK screen displays.	NVVPNPSWDTYPE
		2 of 2

User Password Entry screen

This screen displays to allow you to change your VPN password, if you are permitted to do so. If you already have a VPN password, eight asterisks display. If you do not have a VPN password, the User Password line is blank. Pressing **Change** displays the VPN Text Entry screen, where you can enter a new password or change the current password. Be sure to press **Save** on the Text Entry screen, then press the **Right Arrow** to save the password and move to either the VPN Settings screen (see Viewing or changing settings using the VPN Special Procedure), the IKE PSK screen, or the IKE Phase 1 screen, whichever is applicable to your VPN structure.

IKE PSK screen

This screen lets you view or change two IKE values, the IKE ID (or Group Name) and the Pre-Shared Key (PSK). Pressing **Change** on either line displays the VPN Text Entry screen, where you can enter an IKE ID value or PSK value if there currently is none, or change the current IKE ID or PSK value if one displays. Be sure to press/touch **Save** on the Text Entry screen, then press the **Right Arrow** to save the new or changed value(s) and move to the IKE Phase 1 screen.

IKE Phase 1 screen

This screen lets you view or change Internet Key Exchange Protocol (IKE) values. Press/touch **Change** to change the value, then the **Right Arrow** to display the IKE Phase 2 screen.

Line/Field	Description	Associated System Parameter
IKE ID Type	The following descriptions display, depending on the value of the NVIKEIDTYPE parameter: If the IKE ID Type is 1, "IPV4_ADDR" displays. If the IKE ID Type is 2, "FQDN" displays. If the IKE ID Type is 3 "USER_FQDN" displays. If the IKE ID Type is 9, "DER_ASN1_DN" displays. If the IKE ID Type is 11, "KEY_ID" displays.	NVIKEIDTYPE
IKE Xchg Mode	Aggressive Mode ("1") or ID Protect ("2").	NVIKEXCHGMODE
IKE DH Group	1 denotes First Oakley Group 2 denotes Second Oakley Group 5 denotes 1536-bit MODP Group 14 denotes 2048-bit MODP Group 15 denotes 3072-bit MODP Group	NVIKEDHGRP
	1 of 2	

Line/Field	Description	Associated System Parameter
IKE Encryption Algorithm	0 = Any 1 = AES-128 2 = 3DES 3 = DES 4 = AES-192 5 = AES-256	NVIKEP1ENCALG
IKE Authentication Alg	0 = Any 1 = MD5 2 = SHA	NVIKEP1AUTHALG
IKE Config Mode	Enabled if value is "0" Disabled if value is "1"	NVIKECONFIGMODE
	2 of 2	

IKE Phase 2 screen

Line/Field	Description	Associated System Parameter
IPsec PFS DH Group	This field and the next four fields display only if your VPN meets the conditions for displaying IKE Phase 2. This field specifies the Diffie-Hellman Group to be used for establishing the IPsec SA (also known as PFS). If this value is not "0", a new Diffie-Hellman exchange will be initiated for each IKE Phase 2 Quick Mode exchange, where the proposed DH group will be as specified by the value of NVPFSDHGRP, and the meaning of the values will be the same as those specified above for NVIKEDHGRP.	NVPFSDHGRP
IPsec Encryption Alg	The encryption algorithm to propose for use during IKE Phase 2 negotiation. Values are: 0 = Any 1 = AES-CBC-128 2 = 3DES-CBC 3 = DES-CBC 4 = AES-CBC-192 5 = AES-CBC-256 6 = Null	NVIKEP2ENCALG
IPsec Authentication Alg	The authentication algorithm to propose for use during IKE Phase 2 negotiation. Values are: 0 = Any 1 = MD5 2 = SHA	NVIKEP2AUTHALG
	1 of 2	

Line/Field	Description	Associated System Parameter
Protected Network	Specifies the IP address range that will use the VPN tunnel. Pressing **Change** brings up the VPN Text Entry screen so that you can enter a new IP address.	If a list, the (first) value of NVIPSECSUBNET
IKE over TCP	This field displays only if your VPN meets the conditions for displaying IKE Over TCP. Specifies whether and when to use TCP as a transport protocol for IKE.	NVIKEOVERTCP
	2 of 2	

After viewing or changing the value(s), press/touch the **Right Arrow** to save any change you made and to display either the VPN Settings screen to review all your settings (see Viewing or changing settings using the VPN Special Procedure on page 30, or the IKE Over TCP screen.

IKE Over TCP screen

This screen lets you view or change the IKE Over TCP value, which determines the transport protocol for IKE/ISAKMP.

If the IKE over TCP (NVIKEOVERTCP) value is:	This description displays:
0	Never use TCP as a transport protocol form IKE.
1	Auto; IKE over UDP is tried first; if not successful, IKE over TCP is used.
2	Always use TCP as the transport protocol for IKE.

Pressing **Change** displays the next higher value. Press the **Right Arrow** to save the new or changed value(s) and move to the VPN Settings screen to review all your settings. See Viewing or changing settings using the VPN Special Procedure on page 30 for more information about this all-inclusive screen.

VPN Text Entry screen

When you select a text value on a screen and press/touch **Change**, the VPN Text Entry screen displays the current setting and a blank area for you to enter the new setting. Use the dialpad to enter text, as you would on a cellular phone. The **Symbol** softkey displays an ASCII Symbol Table, from which you can select a symbol.

After entering the new setting, press/touch **Save** to post the entry to the screen from which it came and return to that screen. Then press the **Right Arrow** to save the change and move to the next applicable screen.

IP Address screen

When you select a setting that contains an IP Address and press/touch **Change**, the IP Address screen displays the current setting and a blank area for you to enter the new IP Address. Use the dialpad to enter the IP Address as you would on a cellular phone in the following format: 0.0.0.0 (four numbers separated by decimals, with each number being between 0 and 255). You can use the * (asterisk) key to enter the decimals.

After entering the new IP Address, press/touch **Save** to post the entry to the screen from which it came and return to that screen. Then press the **Right Arrow** to save the change(s) on that screen and move to the next applicable screen.

Chapter 6: User Authentication and VPN Sleep Mode

Introduction

This chapter covers how to enter your user name and password for security authentication and how to activate the sleep mode to terminate/reactivate the VPN connection. Prior to performing any of the procedures in this section, and based on how the remote VPN phones are set up, the administrator should establish appropriate values for VPN tunnel connection and user authentication.

Note:

All 9600 Series IP Telephones except the 9670G require you to select a line or desired action and press a button/softkey to act upon your selection. On 9670G IP Telephones, all actions are touch-based; for example, text/numeric entry uses an on-screen keyboard, and actions are taken or confirmed by touching the applicable line, feature, icon, or softkey on the screen. The procedures that follow apply to non-9670G phones and should be adjusted accordingly for the 9670's touch screen.

User Authentication

VPN User Name Entry screen

This screen displays to validate the user name or to allow an existing user name to be edited if these three conditions are met: NVVPNUSER contains a non-null value (meaning you have a previously assigned user name), the NVVPNPSWD (VPN password) value is null, and the value of NVVPNUSERTYPE is "1" to allow the VPN user to enter or change a user name.

- To accept the user name displayed, press/touch **Enter**.
- To enter a new name or edit the current user name, enter at least one character to display the **VPN User Name Editing screen**.
  - To enter a new name, press/touch **Clear**, then use standard keyboard text entry to enter the new name. Press/touch **Enter** to save the entry as the NVVPNUSER value and to

display either the VPN Password Reuse screen if a password is already stored in memory or the VPN Password Entry screen if a password is not stored in memory.

- To edit the current name, press/touch **Bksp** or **Clear** and use standard text entry to edit the name. Press/touch **Enter** to save the entry as the NVVPNUSER value and display either the VPN Password Reuse screen if a password is already stored in memory or the VPN Password Entry screen if a password is not stored in memory.

VPN Password Reuse screen

This screen displays to authenticate an existing password or to allow access to the VPN Password Entry screen for entry of a new password.

- To accept the current password, press/touch **Enter**. Authentication of the user name and password occurs and if successful, the VPN Tunnel setup screen redisplays. If authentication is unsuccessful, the VPN Authentication Failure screen displays; press/touch **Continue** to reenter the user name and/or password.
- To delete the current password and enter a new password, press/touch **Clear** to display the VPN Password Entry screen. Enter at least one character to display the **VPN User Name Editing screen**, described in the VPN Password Entry screen procedure that follows.

VPN Password Entry screen

This screen displays to allow entry of a new password.

- To enter a new password, enter at least one character to display the **VPN Password Editing screen**.
  - To enter a new password, press/touch **Clear**, then use standard keyboard text entry to enter the new password. Press/touch **Enter** to save the entry as the NVVPNPSWD (VPN Password) value if NVPNPSWDTYPE is "1", or to store the password in volatile memory if NVVPNPSWDTYPE is not "1". Authentication of the user name and password occurs and if successful, the VPN Tunnel setup screen redisplays. If authentication is unsuccessful, the VPN Authentication Failure screen displays; press/touch **Continue** to reenter the user name and/or password.

Note:

When NVPNPSWDTYPE has a value of "3" or "4" the password is deleted from memory immediately after it is used. See Appendix A: VPN Parameters for an explanation of the NVVPNPSWDTYPE values.

VPN Sleep Mode

Your phone connects to your corporate network through a VPN tunnel. If VPN tunnel establishment fails or if an existing VPN tunnel fails, the VPN Tunnel Failure screen displays to notify you of the situation and provide the option to inactivate your phone by putting it into a "sleep mode." Sleep mode also turns the telephone backlight off to conserve energy until the tunnel can be re-established. This section describes sleep mode in relation to VPN tunnel failure, but you can also activate sleep mode from the Login screen or the Unnamed Registration screen. Activating sleep mode can be helpful when the phone is located in a bedroom and an illuminated display would disturb you.

Note:

On 9600 Series IP Telephones, you can touch the **LightOff** softkey at any time to turn off the display backlight, regardless of being connected for VPN operation or not.

When you see the VPN Tunnel Failure screen, the right softkey is labeled **Sleep**. Pressing (or touching if you have a 9670G phone) this softkey turns off the display backlight and displays the message "VPN tunnel terminated." One softkey, **Wake Up**, is available.

Pressing/touching **Wake Up** or pressing/touching any telephone button illuminates the telephone display area and displays two softkeys, **Activate** and **Sleep**:

- The **Activate** softkey initiates VPN tunnel establishment, so that you can use your phone as a remote VPN phone.
- The **Sleep** softkey turns off the backlight and places the telephone back into sleep mode.

Chapter 7: VPN Troubleshooting Guidelines

Introduction

This chapter describes problems that might occur during VPN initialization or operation, and provides possible ways of resolving these problems.

Error and Status Messages

The messages in Table 1 apply to VPN operation only. For messages other than those listed contact your system administrator if you are a VPN user at a remote site. If you are an administrator, see the *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Installation and Maintenance Guide.* Messages display only for about 30 seconds, and then the telephone resets.

Note:

VPN tunnel establishment is retried automatically for failures that may have been caused by a temporary network, server, or gateway outage.

Table 1: Possible Error and Status Messages During VPN Tunnel Connection

Message	Cause/Resolution
`VPN Authentication Failed`	**CAUSE:** Incorrect credentials provided for authentication or not provided at all. **RESOLUTION:** Follow the display prompts and reenter the password.
`VPN Tunnel Failure`	**CAUSE:** The remote telephone cannot establish a link with the VPN tunnel. **RESOLUTION:** Press **Retry** to attempt connection again. If that fails, press **Details** for more information as to why the VPN tunnel could not be established.
`Need gateway IP address`	**CAUSE:** The system parameter NVSGIP is null. **RESOLUTION:** Set NVSGIP to show the IP Address of the VPN security gateway.

1 of 3

Table 1: Possible Error and Status Messages During VPN Tunnel Connection

Message	Cause/Resolution
`Need DNS server IP address`	**CAUSE:** The IP address given for the VPN gateway is a DNS name, but an IP address for a DNS server was not configured. **RESOLUTION:** If the DHCP service in the Internet access device is not providing an IP address for a DNS server, or if DHCP is not being used, an external DNS server IP address must be manually programmed using the local administrative (Craft) VPN procedure.
`Need IKE ID/PSK`	**CAUSE:** The value of system parameter NVPNAUTHTYPE is "3" or "4" indicating a Pre-Shared Key but the value of one or both system parameters NVIKEID or NVIKEPSK is null. **RESOLUTION:** Determine which parameter is null and set a value.
`Need phone certificate`	**CAUSE:** The value of system parameter NVVPNAUTHTYPE is "5" or "7" indicating RSA signature authentication, but a device certificate is not stored in the phone. **RESOLUTION:** Use SCEP to provision a digital certificate in the phone.
`Invalid Configuration`	**CAUSE:** A configuration problem not covered by the preceding five messages. **RESOLUTION:** Review settings and reconfigure values as needed.
`No DNS server response`	**CAUSE:** The DNS server is out of service. **RESOLUTION:** Either wait for the DNS server to come back into service, configure an IP address for an alternate DNS server, or provide dotted-decimal IP addresses for the DNS names that cannot be resolved.
`Bad gateway DNS Name`	**CAUSE:** The DNS server cannot resolve the gateway DNS name. **RESOLUTION:** Check the spelling of the DNS name for the VPN gateway.
`Gateway certificate invalid`	**CAUSE:** The identity certificate presented by the VPN gateway is not valid. **RESOLUTION:** Check whether the TRUSTCERTS parameter has been configured with the name of a file that contains a PEM-format copy of the Certificate Authority (CA) certificate that signed the server's identity certificate; otherwise check whether the server certificate has expired.
`Phone certificate invalid`	**CAUSE:** The VPN gateway has rejected the digital certificate presented by the phone. **RESOLUTION:** Use SCEP to provision a new digital certificate in the phone.
`IKE Phase 1 no response`	**CAUSE:** A message was not received from the VPN gateway in response to a message sent by the phone. Another cause might be that a Phase 1 parameter is not set correctly, causing the VPN gateway to ignore the message from the phone. **RESOLUTION:** Either the VPN gateway is experiencing difficulties, or network congestion is interfering with communication. If that is not the cause, check the following IKE Phase 1 parameters for compatibility: NVVPNSVENDOR, NVVPNAUTHTYPE, NVIKEDHGRP, NVIKEP1AUTHALG, NVIKEP1ENCALG, and NVIKEP1LIFESEC.

2 of 3

Table 1: Possible Error and Status Messages During VPN Tunnel Connection

Message	Cause/Resolution
`IKE ID/PSK invalid`	**CAUSE:** The value in either system parameter NVIKEID or NVIKEPSK is invalid. **RESOLUTION:** Verify that the current value is correct.
`IKE Phase 1 failure`	**CAUSE:** An IKE Security Association could not be established between the phone and the VPN gateway. **RESOLUTION:** Check the following IKE Phase 1 parameters for compatibility: NVIKEDHGRP, NVIKEP1AUTHALG, NVIKEP1ENCALG, and NVIKEP1LIFESEC.
`IKE Phase 2 no response`	**CAUSE:** A message was not received from the VPN gateway in response to a message sent by the phone. Another cause might be that a Phase 2 parameter is not set correctly, causing the VPN gateway to ignore the message from the phone. **RESOLUTION:** Either the VPN gateway is experiencing difficulties, or network congestion is interfering with communication. If that is not the cause, check the following IKE Phase 2 parameters for compatibility: NVIKEP2AUTHALG, NVIKEP2ENCALG, NVIKEP2LIFESEC, and NVPFSDHGRP.
`IKE Phase 2 failure`	**CAUSE:** An IPSec Security Association could not be established between the phone and the VPN gateway. **RESOLUTION:** Check the following IKE Phase 2 parameters for compatibility: NVIKEP2AUTHALG, NVIKEP2ENCALG, NVIKEP2LIFESEC, and NVPFSDHGRP.
`IKE keep-alive failure`	**CAUSE:** A keep-alive message was not received from the VPN gateway for an extended interval. **RESOLUTION:** Either the VPN gateway is experiencing difficulties or network congestion is interfering with communication.
`IKE SA expired`	**CAUSE:** The IKE Security Association was not renewed. **RESOLUTION:** Check the security policy configured in the VPN gateway to ensure that it supports renewals for the desired interval.
`IPSec SA expired`	**CAUSE:** The IPSec Security Association was not renewed. **RESOLUTION:** Check the security policy configured in the VPN gateway to ensure that it supports renewals for the desired interval.
`VPN tunnel terminated`	**CAUSE:** The telephone is in VPN Sleep mode. **RESOLUTION:** Pressing "Wake Up" provides an option to re-activate the VPN tunnel.
`SCEP: Failed`	**CAUSE:** The telephone cannot enroll the certificate using SCEP from the call server. **RESOLUTION:** Check to be sure that the following parameters are configured properly: MYCERTURL, MYCERTCAID, MYCERTCN, MYCERTDN, SCEPPASSWORD, and MYCERTKEYLEN (also check WMLPROXY if the SCEP server is outside of the corporate firewall). If the parameters are properly configured, check that the applicable server is setup and running properly.

3 of 3

Appendix A: VPN Parameters

This appendix describes the system parameters applicable to VPN setup and maintenance, and lists:

- the parameter names,
- their default values,
- the valid values or ranges for those values, and
- a description of each parameter.

Parameter Name	Default Value	Description and Value Range
ALWCLRNOTIFY	0	Specifies whether un-encrypted ISAKMP Notification Payloads will be accepted. One ASCII numeric digit. Valid values are: 0 = Ignore a received Notification Payload that is not encrypted, 1 = Accept a received Notification Payload for further processing.
HTTPPORT	80	TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are “80” through “65535”. Note that when the file server is on Communication Manager, set this value to “81” (port required for HTTP downloads) rather than the using the default.
HTTPSRVR	" " (Null)	IP Address(es) or DNS Name(s) of HTTP file servers used to download telephone files. Dotted decimal or DNS format, separated by commas (0-255 ASCII characters, including commas).
MYCERTCAID	"CAIdentifier"	Certificate Authority Identifier to be used in a certificate request. 0 to 255 ASCII characters.
MYCERTCN	"$SERIALNO"	Common Name of the Subject of a certificate request. 0 to 255 ASCII characters that contain the string "$SERIALNO" or "$MACADDR".
MYCERTDN	" " (Null)	Additional information for the Subject of a certificate request. 0 to 255 ASCII characters
MYCERTKEYLEN	1024	Bit length of the private key to be generated for a certificate request. 4 ASCII numeric digits, "1024" through "2048".
MYCERTRENEW	90	Percentage of a certificate's Validity interval after which renewal procedures will be initiated. 1 or 2 ASCII numeric digits, "1" through "99".
MYCERTURL	" " (Null)	URL to be used to contact an SCEP server. 0 to 255 ASCII characters, zero or one URL.

Parameter Name	Default Value	Description and Value Range
MYCERTWAIT	1	Specifies whether the telephone will wait until a pending certificate request is complete, or whether it will periodically check in the background. 1 ASCII numeric digit, "0" or "1" as follows: 1 = If a connection to the SCEP server is successfully established, SCEP will remain in progress until the request for a certificate is granted or rejected. 0 = SCEP will remain in progress until the request for a certificate is granted or rejected or until a response is received indicating that the request is pending for manual approval.
NORTELAUTH	1	Specifies user authentication method for Nortel security gateways. 1 ASCII numeric digit. Valid values are: 1= Local credentials 2 = RADIUS credentials 3 = RADIUS SecurID 4 = RADIUS Axent
NVHTTPSRVR	0.0.0.0	VPN and non-VPN. HTTP file server IP addresses used to initialize HTTPSRVR the next time the phone starts up. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces. As of Software Release 3.1, NVHTTPSRVR is provided for VPN mode so that a file server IP address can be preconfigured and saved in non-volatile memory.
NVIKECONFIGMODE	1	Enables IKE configuration mode. 1 ASCII numeric digit. Valid values are: 1 = The ISAKMP configuration method will be supported for setting the following values: ● IPADD will be set from a received value of INTERNAL_IP4_ADDRESS, ● the IPADD lease time will be set from a received value of INTERNAL_ADDRESS_EXPIRY, ● DNSSRVR will be set from received value(s) of INTERNAL_IP4_DNS, ● DHCPSRVR will be set from received value(s) of INTERNAL_IP4_DHCP, and ● NVIPSECSUBNET will be set from received value(s) of INTERNAL_IP4_SUBNET 2 = Disable/turn off this setting because a generic PSK profile is in effect.

Parameter Name	Default Value	Description and Value Range
NVIKEDHGRP	2	Specifies the Diffie-Hellman Group to be used for establishing the IKE SA. 1 or 2 ASCII numeric digits. Valid values are: 1 = First Oakley Group 2 = Second Oakley Group 5 = 1536-bit MODP Group 14 = 2048-bit MODP Group 15 = 3072-bit MODP Group For more information, see Section 4 in RFC 3526.
NVIKEID	"VPNPHONE"	Specifies the identity to be used during IKE Phase 1 negotiation (also called the group name in XAUTH). 0 to 30 ASCII characters.
NVIKEIDTYPE	3	Specifies the type of identification to use for establishing the IKE SA. 1 or 2 ASCII numeric digits. Valid values are: 1 = ID_IPV4_ADDR 2 = ID_FQDN 3 = ID_USER_FQDN 9 = ID_DER_ASN1_DN 11= ID_KEY_ID
NVIKEOVERTCP	0	Specifies whether and when to use TCP as a transport protocol for IKE. 1 ASCII numeric digit. Valid values are: 0 = Never use TCP as a transport protocol for IKE. 1 = Auto; use IKE over UDP first, and if that isn't valid use IKE over TCP. 2 = Always use TCP as the transport protocol for IKE.
NVIKEP1AUTHALG	0	Specifies the authentication algorithm to use during IKE Phase 1 negotiation. 1 ASCII numeric digit. Valid values are: 0 = Any 1 = MD5 (per RFC 2403) 2 = SHA (per RFC 2404)
NVIKEP1ENCALG	0	Specifies the encryption algorithm to use during IKE Phase 1 negotiation. 1 ASCII numeric digit. Valid values are: 1 = AES-CBC-128 (per RFC 3602) 2 = 3DES-CBC (per RFC 2451) 3 = DES-CBC (per RFC 2405) 4 = AES-CBC-192 (per RFC 3602) 5 = AES-CBC-256 (per RFC 3602)
NVIKEP1LIFESEC	432000	Specifies the IKE SA lifetime in seconds. 3 to 8 ASCII numeric digits. Valid values are: "600" through "15552000".

3 of 7

Parameter Name	Default Value	Description and Value Range
NVIKEP2AUTHALG	0	Specifies the authentication algorithm to use during IKE Phase 2 negotiation. 1 ASCII numeric digit. Valid values are: 0 = Any 1 = MD5 (per RFC 2403) 2 = SHA (per RFC 2404)
NVIKEP2ENCALG	0	Specifies the encryption algorithm to use during IKE Phase 2 negotiation. 1 ASCII numeric digit. Valid values are: 0 = Any 1 = AES-CBC-128 (per RFC 3602) 2 = 3DES-CBC (per RFC 2451) 3 = DES-CBC (per RFC 2405) 4 = AES-CBC-192 (per RFC 3602) 5 = AES-CBC-256 (per RFC 3602) 6 = Null
NVIKEP2LIFESEC	432000	Specifies the IPsec SA lifetime in seconds. 3 to 8 ASCII numeric digits. Valid values are: "600" through "15552000".
NVIKEPSK	" " (Null)	Specifies the pre-shared key to be used during IKE Phase 1 negotiation (also called the group password in XAUTH. Zero to 30 ASCII characters.
NVIKEXCHGMODE	1	Specifies the IKE Phase 1 negotiation mode. 1 ASCII numeric digit.Valid values are: 1 = Aggressive Mode. 2 = Main Mode Identity Protection. (Per Section 5 in RFC 2409.)
NVIPSECSUBNET	0.0.0.0/0	Specifies IP address ranges that will use the VPN tunnel. 0 to 255 ASCII characters: zero or more dotted decimal IP address/integer strings, separated by commas without any intervening spaces.
NVMCIPADD	0.0.0.0	Call server IP Addresses. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
NVPFSDHGRP	0	Specifies the Diffie-Hellman Group to be used for establishing the IPsec SA (also known as PFS). 1 or 2 ASCII numeric digits. Valid values are: 1 = First Oakley Group 2 = Second Oakley Group 5 = 1536-bit MODP Group 14 = 2048-bit MODP Group 15 = 3072-bit MODP Group For more information, see Section 4 in RFC 3526.
NVSGIP	" " (Null)	VPN security gateway IP addresses. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.

Parameter Name	Default Value	Description and Value Range
NVTLSSRVR	0.0.0.0	VPN and non-VPN. HTTPS file server IP addresses used to initialize TLSSRVR the next time the phone starts up. 0 to 255 ASCII characters: zero or more IP addresses in dotted decimal or DNS name format, separated by commas without any intervening spaces.
NVVPNAUTHTYPE	3	Specifies the user authentication method. 1 ASCII numeric digit. Valid values are: 3 = Pre-Shared Key (PSK) 4 = PSK with XAUTH 5 = RSA signatures with XAUTH 6 = Hybrid XAUTH 7 = RSA Signatures
NVVPNCFGPROF	0	VPN configuration profile. 1 or 2 ASCII numeric digits. Valid values are: "0", "1", "2", "3", "5", "6", "8", "9" or "11". See VPN Configuration Profiles for information and a description of valid values.
NVVPNCOPYTOS	2	Specifies whether to copy the TOS bits from the tunneled (inner) IP header to the tunnel (outer) IP header. 1 ASCII numeric digit. Values are: 1 = the value of the TOS bits will be copied from the inner IP header to the outer IP header. 2 = the TOS bits of the outer IP header will be set to 0.
NVVPNENCAPS	0	Specifies port numbers used for IKE and IPsec UDP encapsulation, and support for NAT traversal. 1 ASCII numeric digit. Valid values are: 0 = Procedures for the negotiation of NAT traversal will be supported as specified in IETF RFC 3947, except that IKE negotiation will begin with a source port of 2070 (instead of 500), and that source port will continue to be used unless the source and destination port numbers are changed to 4500 per RFC 3947. 1 = UDP encapsulation of the "inner" IP layer will not be provided. The procedures for the negotiation of NAT traversal specified in IETF RFC 3947 will not be supported. 2 = Procedures for the negotiation of NAT traversal will be supported as specified in IETF RFC 3947, except that IKE will use a source port of 2070, and the source and destination port numbers will not be subsequently changed. UDP encapsulation of the "inner" IP layer will be supported as specified in RFC 3948 [7.3-41c], using the same UDP source and destination port numbers that were used during the final phase of IKE 4 = Procedures for the negotiation of NAT traversal will be supported as specified in IETF RFC 3947. UDP encapsulation of the "inner" IP layer will be supported as specified in RFC 3948 [7.3-41c], using the same UDP source and destination port numbers that were used during the final phase of IKE

Parameter Name	Default Value	Description and Value Range
NVVPNMODE	0	Specifies whether VPN is supported. 1 ASCII numeric digit. Valid values are: 0 = VPN is not supported. 1 = VPN is supported. Also see DHCPACK Messages for additional information.
NVVPNPSWD	" " (Null)	User password for VPN. If the user password can be stored in NV memory (see NVVPNPSWDTYPE below), it is stored as the value of NVVPNPSWD. 0 to 16 ASCII characters.
NVVPNPSWDTYPE	1	Specifies whether and how the VPN user password will be stored. 1 ASCII numeric digit. Valid values are: 1 = Password can be alphanumeric and is stored in reprogrammable non-volatile memory as the NVVPNPSWD value. 2 = Password can be alphanumeric and is stored in volatile memory but will be cleared when the phone resets. 3 = Password can be numeric only and is stored in volatile memory that is cleared immediately after first-time password use. 4 = Password can be alphanumeric and is stored in volatile memory that is cleared immediately after first-time password use. 5 = Password can be alphanumeric and is stored in volatile memory that is cleared when the user invokes VPN Sleep Mode and when the telephone resets.
NVVPNSVENDOR	4	Specifies the IKE implementation to use. 1 ASCII numeric digit. Valid values are: 1 = Juniper PSK with XAUTH or Juniper Cert with XAUTH 2 = Cisco PSK with XAUTH or Cisco Cert with XAUTH 3 = Checkpoint Security Gateway 4 = Generic PSK 5 = Nortel Contivity See VPN Configuration Profiles for information on automatically-set parameters based on this NVVPNSVENDOR setting.
NVVPNUSER	" " (Null)	Specifies the user name to use during authentication. 0 to 16 ASCII characters.
NVVPNUSERTYPE	1	Specifies whether the user can change the VPN username. 1 ASCII numeric digit. Valid values are: 1 = User can change VPN user name 2 = User cannot change VPN user name

6 of 7

Parameter Name	Default Value	Description and Value Range
NVXAUTH	1	Specifies whether to disable XAUTH user authentication for profiles that enable XAUTH by default. 1 ASCII numeric digit. Valid values are: 1= XAUTH user authentication enabled 2 = XAUTH user authentication disabled
SCEPPASSWORD	"$SERIALNO"	Specifies a challenge password for SCEP. Zero to 32 ASCII characters
TLSPORT	411	TCP port number used for HTTP file downloading. 2 to 5 ASCII numeric digits. Valid values are "80" through "65535".
TLSSRVRID	1	Controls whether the identity of a TLS server is checked against its certificate. 1 ASCII numeric digit. Valid values are: 1=Provides additional security by checking to verify that the server certificate's DNS name matches the DNS name used to contact the server. 0=Certificate is not checked against the DNS name used to contact the server.
VPNACTIVE	0	Indicates whether a VPN tunnel has been established. Valid values are: 0 = VPN tunnel not established. 1 = VPN tunnel established. If an existing VPN tunnel fails, VPNACTIVE will be set to "0", IPADD will be set to "0.0.0.0", DNSSRVR will be set to the value of EXTDNSSRVR, DOMAIN will be set to null, the backlight will be turned on, the display will be cleared, and the name/logo image will be displayed. Also see DHCPACK Messages for additional information.
VPNCODE	876	VPN procedure access code; default is "VPN" on the dialpad. Zero to 7 ASCII numeric digits, null ("") and "0" through "9999999".
VPNPROC	1	Specifies whether VPNCODE can be used to access the VPN procedure at all, in view-only mode, or in view/modify mode. 1 ASCII numeric digit. Valid values are: 0 = User cannot access VPN settings/information. 1= The user can view the VPN Settings Screen but cannot change VPN settings. 2 = User has the ability to view and change VPN settings.
VPNTTS	0	Turns off Time to Service (TTS) support when a VPN gateway may not allow TTS functionality to work. Valid values are: 0 = TTS is not supported by the security gateway; turn off TTS functionality for VPN operation. 1 = TTS is supported by the security gateway; VPN operation will support TTS functionality.

7 of 7

VPN Configuration Profiles

Based on the value of NVVPNCFGPROF, the other persistent parameters listed inTable 2 below will automatically be set to the value specified Column 2. If a value is not specified for a persistent parameter in the table below, the value of the parameter will not be changed. If the value of NVVPNCFGPROF is "0", no values will be set for the other persistent parameters shown here.

The administrator can set any of the parameters listed individually, however allowing them to be set automatically ensures that related settings are correct.

Table 2: Security Gateway System Parameters

Supported Device as set by the administrator	System Parameter Values (set automatically)
Checkpoint Security Gateway (NVVPNCFGPROF = 2)	Sets the following values (to): **NVIKECONFIGMODE(1)** **NVIKEID ("" - Null String)** **NVIKETYPE (11)** **NVIKEOVERTCP(1)** **NVIKEXCHANGEMODE(2)** **NVVPNAUTHTYPE (6)** **NVVPNSVENDOR (3)**
Cisco PSK with XAUTH (NVVPNCFGPROF = 3)	Sets the following values (to): **NVIKECONFIGMODE(1)** **NVIKEID ("" - Null String)** **NVIKETYPE (11)** **NVIKEXCHANGEMODE(1)** **NVVPNAUTHTYPE (4)** **NVVPNSVENDOR (2)**
Cisco Cert with XAUTH (NVVPNCFGPROF = 8)	Sets the following values (to): **NVIKECONFIGMODE(1)** **NVIKEID ("" - Null String)** **NVIKETYPE (11)** **NVIKEXCHANGEMODE(1)** **NVVPNAUTHTYPE (5)** **NVVPNSVENDOR (2)**
Juniper PSK with XAUTH (NVVPNCFGPROF = 5)	Sets the following values (to): **NVIKECONFIGMODE(1)** **NVIKEID ("" - Null String)** **NVIKETYPE (3)** **NVIKEXCHANGEMODE(1)** **NVVPNAUTHTYPE (4)** **NVVPNSVENDOR (1)**

1 of 2

Table 2: Security Gateway System Parameters (continued)

Supported Device as set by the administrator	System Parameter Values (set automatically)
Juniper Cert with XAUTH (NVVPNCFGPROF = 9)	Sets the following values (to): **NVIKECONFIGMODE(1)** **NVIKEID ("" - Null String)** **NVIKETYPE (9)** **NVIKEXCHANGEMODE(1)** **NVVPNAUTHTYPE (5)** **NVVPNSVENDOR (1)**
Nortel Contivity (NVVPNCFGPROF = 11)	Sets the following values (to): **NVIKECONFIGMODE(1)** **NVIKEID ("" - Null String)** **NVIKETYPE (11)** **NVIKEXCHANGEMODE(1)** **NVVPNAUTHTYPE (3)** **NVVPNSVENDOR (5)**
Any Security Device (Generic) with Preshared Key (PSK) (NVVPNCFGPROF = 6)	Sets the following values (to): **NVIKECONFIGMODE(2)** **NVIKEID ("" - Null String)** **NVIKETYPE (3)** **NVIKEXCHANGEMODE(1)** **NVVPNAUTHTYPE (3)** **NVVPNSVENDOR (4)**
	2 of 2

DHCPACK Messages

If the value of NVVPNMODE is "1" and the value of VPNACTIVE is "0", the values of the following parameters will be set based on the fields and options received in the DHCPACK message when DHCP is in the INIT state (converting from binary to ASCII as necessary):

- The parameter EXTIPADD will be set to the value of the yiaddr field,
- The parameter EXTNETMASK will be set to the value of option #1 (if received),
- The parameter EXTGIPADD will be set to the first value of option #3 (if received, which may be a list of IP addresses),
- The parameters DNSSRVR and EXTDNSSRVR will be set to the value of option #6 (if received, which may be a list of IP addresses),
- The DHCP lease time for EXTIPADD will be set to the value of option #51 (if received),
- The DHCP lease renew time for EXTIPADD will be set to the value of option #58 (if received),

- The DHCP lease rebind time for EXTIPADD will be set to the value of option #59 (if received).

If the value of NVVPNMODE is "1" and the value of VPNACTIVE is "1", the values of the following parameters will be set based on the fields and options received in the DHCPACK message (converting from binary to ASCII as necessary):

- The parameters TLSSRVR and HTTPSRVR will be set to the value of the siaddr field if and only if the siaddr field is non-zero,
- The parameter DNSSRVR will be set to the value of option #6 (if received, which may be a list of IP addresses), and
- The parameter DOMAIN will be set to the value of option #15 (if received).

Time to Service (TTS) Functionality

Important:

Some vendors may have gateways that interfere with TTS functionality. Avaya recommends always setting the system parameter VPNTTS to "1" (On) unless you determine that your gateway interferes with TTS. If you determine that your gateway interferes with TTS, set or leave the VPNTTS default of "0" (Off), which turns off TTS.

Appendix B: Glossary of Terms

Terms Used in This Guide

This appendix lists terms used in this guide or of interest to new VPN users.

CA	Certificate Authority; the entity which issues digital certificates for use by other parties.
Diffie -Hellman key exchange	A key agreement algorithm based on the use of two public parameters p and g that may be used by all users in a system. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p.
DH Group	A number that determines the public parameters used by the Diffie-Hellman key exchange. To successfully establish a shared secret key, the same DH group must be used by both parties.
Digital Certificate	The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by a trusted third party known as a "Certificate Authority" (CA) such as VeriSign (www.verisign.com). The CA verifies that a public key belongs to a specific company or individual (the "Subject"), and the validation process it goes through to determine if the subject is who it claims to be depends on the level of certification and the CA itself.
Digital Signature	A digital signature is an encrypted digest of the file (message, document, driver, program) being signed. The digest is computed from the contents of the file by a one-way hash function such as MD5 or SHA-1 and then encrypted with the private part of a public/private key pair. To prove that the file was not tampered with, the recipient uses the public key to decrypt the signature back into the original digest, recomputes a new digest from the transmitted file and compares the two to see if they match. If they do, the file has not been altered in transit by an attacker.
HTTP	Hypertext Transfer Protocol, used to request and transmit pages on the World Wide Web.
HTTPS	A secure version of HTTP.
IETF	Internet Engineering Task Force, the organization that produces standards for communications on the internet.
IKE	Internet Key Exchange Protocol, RFC 2409, which has been obsoleted by IKEv2 in RFC 4306.

IPsec	A security mechanism for IP that provides encryption, integrity assurance, and authentication of data.
ISAKMP	Internet Security Association and Key Management Protocol, RFC 2408, which has been obsoleted by IKEv2 in RFC 4306, defines the procedures for authenticating a communicating peer, creation and management of security associations, key generation techniques, and threat mitigation e.g. Denial of service and Replay Attacks. ISAKMP defines two phases of negotiation. During Phase 1 negotiation, two entities establish an ISAKMP SA, which is used to protect Phase 2 negotiations, in which SAs are established for other protocols.
Refresh/ Rekey	Use IKE to create a new SA with a new SPI.
RSA	Rivest-Shamir-Adleman; a highly secure asymmetric cryptography method developed by RSA Security, Inc. that uses a public/private key pair. The private key is kept secret by the owner and the public key is published, usually in a digital certificate. Data is encrypted using the recipient's public key, which can only be decrypted by the recipient's private key. RSA is very computation intensive, thus it is often used to encrypt a symmetric session key that is then used by a less computationally-intensive algorithm to encrypt protocol data during a "session". RSA can also be used for authentication by creating a digital signature, for which the sender's private key is used for encryption, and the sender's public key is used for decryption.
RTP	Real-time Transport Protocol. Provides end-to-end services for real-time data such as voice over IP.
SA	Security Association, a security protocol (e.g., IPSec, TLS) and a specific set of parameters that completely define the services and mechanism necessary to protect security at that security protocol location. These parameters can include algorithm identifiers, modes, cryptographic keys, etc. The SA is referred to by its associated security protocol (for example "ISAKMP SA", "ESP SA", "TLS SA").
SCEP	Simple Certificate Enrollment Protocol, used to obtain a unique digital certificate.
SDP	Session Description Protocol. A well-defined format for conveying sufficient information to discover and participate in a multimedia session.
Signaling Channel Encryption	Encryption of the signaling protocol exchanged between the IP telephone and the call server. Signaling channel encryption provides additional security to the security provided by media channel encryption.
SNTP	Simple Network Time Protocol. An adaptation of the Network Time Protocol used to synchronize computer clocks in the internet.
SOHO	Small Office Home Office. The environment for which a virtual private network (VPN) would be administered.
SPD	Security Policy Database. Specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or security gateway IPsec implementation.
SPI	Security Parameter Index. An identifier for a Security Association, relative to some security protocol. Each security protocol has its own "SPI-space".

2 of 3

SRTCP	Secure Real-time Transport Control Protocol.
SRTP	Secure Real-time Transport Protocol.
system -specific	Specific to a particular type of call server, e.g., Avaya Communication Manager (CM) or SIP Enablement Services (SES). "System-specific signaling" refers to messages specific to the signaling protocol used by the system, e.g., H.323 and/or CCMS messages used by CM and IP Office, or SIP messages (possibly including system-specific headers) used by SES. "System-specific procedures" refers to procedures in telephone software that are specific to the call server with which the software is intended to be used.
TCP/IP	Transmission Control Protocol/Internet Protocol, a network-layer protocol used on LANs and internets.
TFTP	Trivial File Transfer Protocol, used to provide downloading of upgrade scripts and application files to certain IP telephones.
TLS	Transport Layer Security, an enhancement of Secure Sockets Layer (SSL). TLS is compatible with SSL 3.0 and allows for privacy and data integrity between two communicating applications.
URI & URL	Uniform Resource Identifier and Uniform Resource Locator. Names for the strings used to reference resources on the Internet (for example, HTTP://....). URI is the newer term.
VPN	Virtual Private Network; a private network constructed across a public network such as the Internet. A VPN can be made secure, even though it is using existing Internet connections to carry data communication. Security measures involve encrypting data before sending it across the Internet and decrypting the data at the other end. An additional level of security can be added by encrypting the originating and receiving network address.

3 of 3

Index

T

U

V