vtech®

ErisTerminal® SIP DECT Base Station VSP600

Administrator and Provisioning Manual

Rev. 9 6/16

CONTENTS

PREFACE

Congratulations on your purchase of this VTech product. Please thoroughly read this manual for all the feature operations and troubleshooting information necessary to install and operate your new VTech product. You can also visit our website at *businessphones.vtech.com* or call **1 (888) 370-2006**.

This administrator and provisioning manual contains detailed instructions for installing and configuring your VSP600 SIP DECT base station with software version 1.1.4 or newer. See *"Using the Status menu" on page 16* for instructions on checking the software version on the VSP600. Please read this manual before installing the product.

Please print this page and record the following information regarding your product:

Model number: VSP600

Type: Small to medium business SIP-endpoint base station

Serial number: _____

Purchase date: _____

Place of purchase: _____

Both the model and serial numbers of your VTech product can be found on the bottom of the console.

Save your sales receipt and original packaging in case it is necessary to return your telephone for warranty service.

Text Conventions

Table 1 lists text formats and describes how they are used in this guide.

Table 1. Description of Text Conventions

Text Format	Description
Screen	Identifies text that appears on a device screen or a WebUI page in a title, menu, or prompt.
HARD KEY or **DIAL-PAD KEY**	Identifies a hard key, including the dial-pad keys.
CallFwd	Identifies a soft key.
NOTE Notes provide important information about a feature or procedure.	Example of a Note.
CAUTION *A caution means that loss of data or unintended circumstances may result.*	Example of a Caution.

Audience

This guide is written for installers and system administrators. It assumes that you are familiar with networks and VoIP, both in theory and in practice. This guide also assumes that you have ordered your IP PBX equipment or service and selected which PBX features you want to implement. This guide references specific IP PBX equipment or services only for features or settings that have been designed for a specific service. Please consult your equipment supplier or service provider for recommended switches, routers, and firewall and NAT traversal settings, and so on.

As the VSP600 SIP DECT base station becomes certified for IP PBX equipment or services, VTech may publish interop guides for those specific services. The interop guides will recommend second-party devices and settings, along with VSP600-specific configurations for optimal performance with those services. For the latest updates, visit our website at *businessphones.vtech.com*.

Related Documents

The ***VSP600 Quick Start Guide*** contains a quick reference guide to the VSP600 external features and brief instructions on connecting the VSP600 to a working IP PBX system.

The ***VSP600 User Guide*** contains a quick reference guide, full installation instructions, instructions for making and receiving calls, and a guide to all user-configurable settings.

The documents are available from our website at *businessphones.vtech.com*.

CHAPTER 1

INTRODUCING THE VSP600

This administrator and provisioning guide contains detailed instructions for configuring the VSP600 SIP DECT base station. Please read this guide before attempting to configure the VSP600.

Some of the configuration tasks described in this chapter are duplicated in the Web User Interface (WebUI) described in the next chapter, but if you need to assign static IP addresses, they must be set at each device.

This chapter covers:

About the VSP600 base station

The VTech VSP600 SIP DECT base station with VSP601cordless handset is a cordless business phone system designed to work with popular SIP telephone (IP PBX) equipment and services. Once you have ordered and configured your SIP equipment or service, the VSP600 and cordless accessories enable you to make and receive calls as you would with any other business phone.

The VSP600 base station features include:

- Up to 6 SIP account registrations
- Up to 4 active SIP sessions (across all handsets and cordless desksets)
- Registration of up to 6 DECT cordless handsets
- Power over Ethernet
- Handset locator

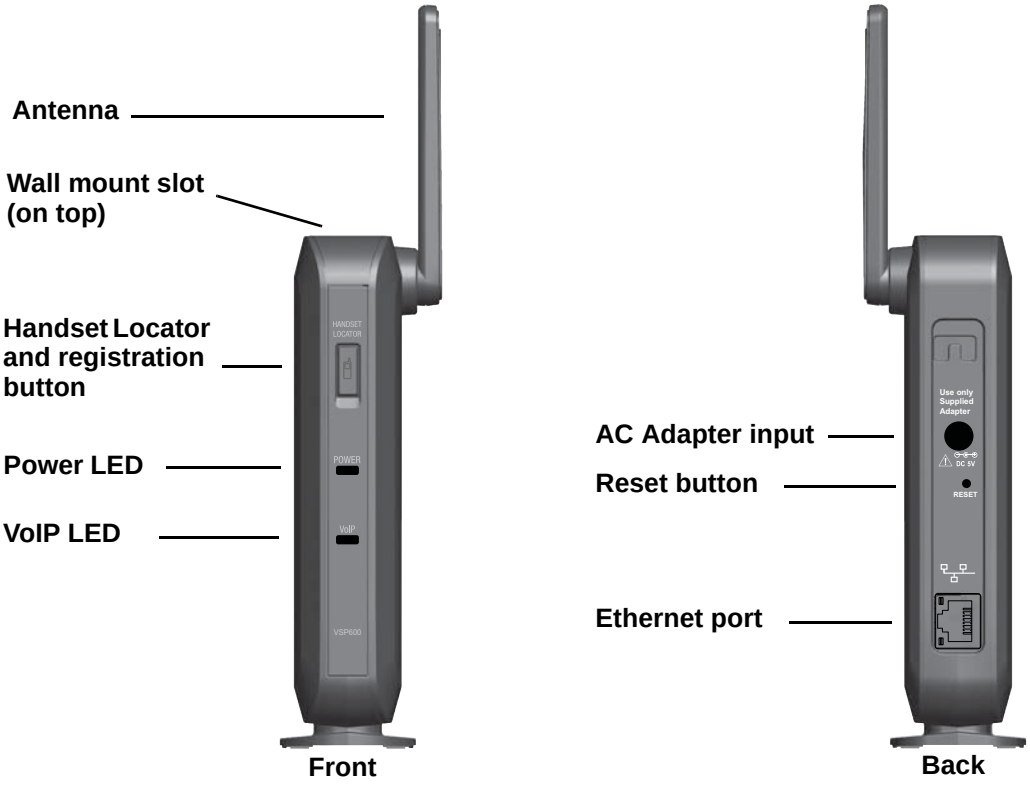
The VSP601 cordless handset features include:

- Orbitlink Wireless Technology™
- Backlit Liquid Crystal Display
- Speakerphone, hold, intercom and mute capability
- Corded headset jack
- 3-way conferencing
- 200-entry call history

You can configure the VSP600 using the menus on the VSP601 handset, a browser-based interface called the WebUI, or an automatic provisioning process (see *"Provisioning Using Configuration Files" on page 73*). The WebUI enables you to configure the VSP600 using a computer that is connected to the same Local Area Network. The WebUI resides on the VSP600, and may get updated with firmware updates.

Quick Reference Guide

The external features of the VSP600 base station and handset are described below.




Message LED
Soft keys
Headset jack
On back of handset:
· Belt clip
· Speaker
For information about the handset call management keys, see the User Guide.
vtech
TRANSFER
CONF.
MENU SELECT
TALK
HOLD
INT
vtech

Network Requirements

A switched network topology is recommended for your LAN (using standard 10/100 Ethernet switches that carry traffic at a nominal rate of 100 Mbit/s).

The office LAN infrastructure should use Cat.-5/Cat.-5e cable.

The VSP600 requires a wired connection to the LAN. However, wireless connections from your LAN to other devices (such as laptops) in your office will not impede performance.

A Dynamic Host Configuration Protocol (DHCP) server is recommended and must be on the same subnet as the VSP600 base stations so that IP addresses can be auto-assigned. In most cases, your network router will have a DHCP server. By default, the VSP600 has DHCP enabled for automatic IP address assignment.

NOTE

Some DHCP servers have default settings that limit the number of network IP addresses assigned to devices on the network. You should log in to your server to confirm that the IP range is sufficient.

If no DHCP server is present, you can assign a static IP to the VSP600. You can assign a static IP address using the VSP600 menu. Go to **Admin settings > Network setting > Set static IP**. If you do not have a DHCP server or do not manually assign static IPs, you will not be able to access the WebUI and/or enable automatic time updates from an NTP server.

A DNS server is recommended to resolve the path to the Internet and to a server for firmware and configuration updates. If necessary, the system administrator can also download upgrade files and use the WebUI to update the VSP600 firmware and/or configuration settings manually.

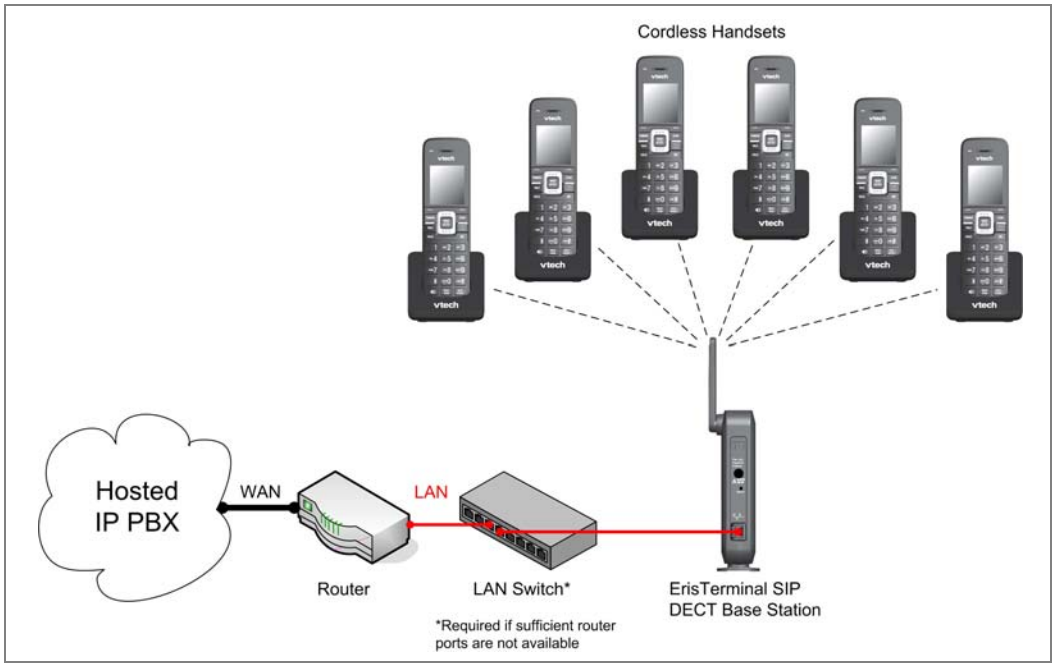


Figure 1. VSP600 Installation Example

VSP600 Configuration Methods

You can configure the VSP600 using one of the following methods:

- From the VSP601 handset, using the handset menus. The VSP601 menus are best suited to configuring a few settings, perhaps after the initial setup has been done. For administrators, the settings available on the VSP601 menus include network settings, account settings, and provisioning settings. See *"Using the Admin Settings Menu" on page 19*. Many of the settings accessible on the VSP601 are most useful for end users. Through the menu, they can customize the screen appearance, sounds, and manage calls. For more information, see the VSP600/VSP601 User Guide.
- The Web User Interface, or WebUI, which you access using your Internet browser. See *"Using the WebUI" on page 25*. The browser-based interface is easy to navigate and best suited to configuring a large number of VSP600 settings at once. The WebUI gives you access to every setting required for configuring a single device. You can enter service provider account settings on the WebUI, assign accounts to handsets, and set up provisioning, which will allow you to automatically and remotely update the VSP600 after initial configuration.
- Provisioning using configuration files. Working with configuration files allows you to configure the device at regular intervals. There are several methods available to enable the VSP600 to locate and upload the configuration file. For example, you can enable the VSP600, when it starts up or reboots, to check for the presence of a configuration file on a provisioning server. If the configuration file is new or has been modified in any way, the VSP600 automatically downloads the file and applies the new settings. For more information, see *"Provisioning Using Configuration Files" on page 73*.

CHAPTER 2

CONFIGURATION USING THE PHONE MENUS

The VSP600 Main Menu has the following sub-menus:

- Message—access the voice messages on each account.
- Directory—view and dial directory and blacklist entries.
- Call history—view missed calls, received calls and dialed calls.
- Intercom—call other handsets.
- Speed dial—view and edit speed dial entries.
- Features—set DND, call forward settings and other calling features.
- Status—view the handset and base station network status, account registration status, and product information.
- User settings—allows the user to set the language for the display, configure the appearance of the display, set date and time, and customize the audio settings.
- Admin settings—configure network settings (enter static IP addresses, for example), account settings and provisioning settings.

This chapter contains instructions for using the Admin Settings menu and for accessing the Status menu. See the VSP600/VSP601 User Guide for more information about the other menus.

Viewing the Main Menu

To use the VSP601 menu:

1. When the VSP601 is idle, press **MENU/SELECT**.
   The **Main Menu** appears.

2. Press ▼ or ▲ to highlight the desired sub-menu, and then press **MENU/SELECT**.
   - Press **SELECT** or an appropriate soft key to save changes.
   - Press **OFF/CANCEL** to cancel an operation, exit the menu display or return to the idle screen.

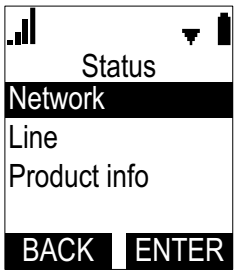
Using the Status menu

Use the **Status** menu to verify network settings and begin troubleshooting if network problems or account registration issues affect operation.

You can also find the software version of the VSP600 on the **Product Info** screen, available from the **Status** menu.

To view the Status menu:

1. When the VSP601 is idle, press **MENU/SELECT**.
2. On the **Main Menu**, press ▲ or ▼ to highlight **Status**, and then press **MENU/SELECT**.
   The **Status** menu appears.



3. On the **Status** menu, press ▲ or ▼ to highlight the desired menu, and then press **MENU/SELECT**.

The available status menus are listed in Table 2.

Table 2. Status menu summary

Menu	Information listed
1. Network	■ IP address ■ DHCP status (Enabled/Disabled) ■ Subnet Mask ■ Gateway IP address ■ DNS server 1 IP address ■ DNS server 2 IP address
2. Line	Lines and registration status. On the **Line** menu, highlight and select the desired line to view detailed line status information: ■ Line status (Registered/Not registered) ■ Account display name ■ Account User ID ■ Server IP address

Table 2. Status menu summary

Menu	Information listed
3. Product Info	Shows the product info for the handset or base station. Select **Handset** or **Base** to view the: ■ Model number (Handset only) ■ Serial number (Handset only) ■ Firmware version ■ V-Series ■ Hardware version

Viewing Line status

To view line status, from the **Status** menu, select **Line**. The **Line** menu lists the available lines, along with icons indicating each line's current registration status.

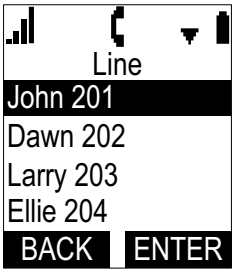
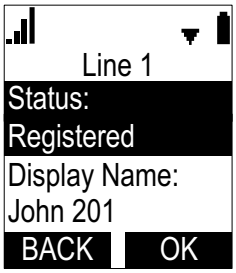


Table 3. Line status icons

Icon	Description
	Line registered
	Line unregistered
	Line disabled

To view complete status information for a line:

- On the **Line** menu, press ▲ or ▼ to highlight the desired line, and then press **MENU/SELECT**. The full line status screen appears.

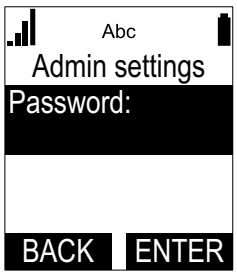


Using the Admin Settings Menu

To access the Admin Settings menu:

1. When the VSP601 is idle, press **MENU/SELECT**.
   The **Main Menu** appears.

2. Press ▲ or ▼ to highlight **Admin settings**, and then press **MENU/SELECT**.
3. Use the dial pad to enter the admin password, and then press **ENTER** . The default password is **admin** (press the * key to enable entering lower-case letters).



The Admin settings are listed in Table 4.

Table 4. Admin setting summary

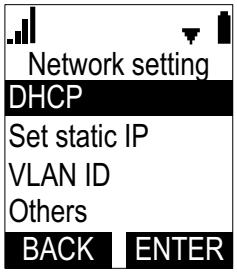
Setting	Options
Network setting	DHCP (Enable, Disable) Set static IP VLAN ID Others
Secure browsing	HTTPs (Enabled, Disabled)
Provisioning	Server string Login ID Login password
Edit PIN code	Edit PIN
Firmware update	Select **Firmware update** to have the handset check whether a firmware update is available. See *"Updating a Cordless Handset" on page 61*.

Using the Network Setting menu

Use the Network setting menu to configure network-related settings for the VSP600. For more information about these settings, see *"Basic Network Settings" on page 45* and *"Advanced Network Settings" on page 46*.

To use the Network setting menu:

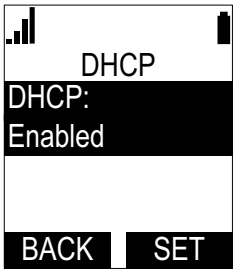
1. From the **Admin Settings** menu, press ▲ or ▼ to highlight **Network setting**, and then press **MENU/SELECT**.
   The **Network setting** menu appears.



2. Press ▲ or ▼ to highlight the desired option, and then press **MENU/SELECT**:
   - DHCP
   - Set static IP
   - VLAN ID
   - Others (DNS and NTP servers).

To enable or disable DHCP:

1. From the **Network setting** menu, press ▲ or ▼ to highlight **DHCP**, and then press **MENU/SELECT**.
   The **DHCP** screen appears.



2. Press **MENU/SELECT** to select **Enabled** or **Disabled**, and then press **SET**.

DHCP is enabled by default, which means the VSP600 will get its IP address from the network. When DHCP is disabled, you must enter a static IP address for the VSP600.

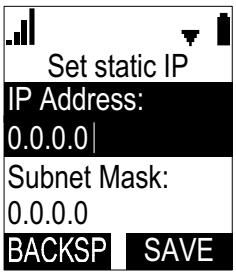
NOTE You must be familiar with TCP/IP principles and protocols to configure static IP settings.

To set static IP for the VSP600:

1. From the **Network setting** menu, press ▲ or ▼ to highlight **Set static IP**, and then press **MENU/SELECT**.

   If DHCP is disabled, the **Set static IP** menu appears. If DHCP is enabled, an error message appears briefly before returning you to the **Network setting** menu.

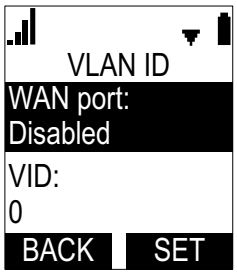
2. On the **Set static IP** menu, enter the static IP address. Use the dial pad to enter characters. To add a period, press the * key.



3. Press ▼ and enter the Subnet Mask. Use the dial pad to enter characters.
4. Press ▼ and enter the Gateway. Use the dial pad to enter characters.
5. Press **SAVE** .

To set the VLAN ID for the VSP600:

1. From the **Network setting** menu, press ▲ or ▼ to highlight **VLAN ID**, and then press **MENU/SELECT**.
2. On the **VLAN ID** menu, press **MENU/SELECT** to enable or disable the WAN Port.

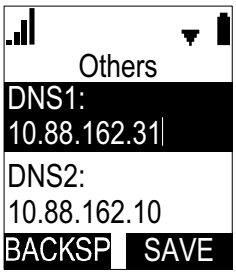


3. Press ▼ and enter the WAN VID. Use the dial pad and the **BACKSP** soft key to enter characters. The valid range is 0 to 4095.
4. Press ▼ and enter the WAN priority. The valid range is 0 to 7.
5. Press **SAVE**.

To set other settings (DNS and NTP):

1. From the **Network setting** menu, press ▲ or ▼ to highlight **Others**, and then press **SELECT**.

   If DHCP is disabled, the **Others** menu appears. If DHCP is enabled, an error message appears briefly before returning you to the **Network setting** menu.

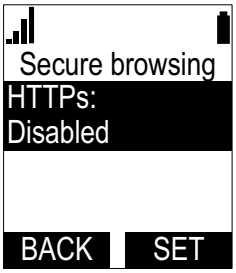


2. Enter the IP address for the primary DNS server. Use the dial pad to enter characters. To add a period, press the * key.
3. Press ▼ and enter the IP address for the secondary DNS server. The VSP600 uses this server if the primary server does not respond.
4. Press ▼ and enter the IP address for the NTP server. If the VSP600 does not use an NTP server, you must manually enter the time and date settings.
5. Press **SAVE**.

Using the Secure browsing menu

To turn on secure browsing:

1. From the **Network setting** menu, press ▲ or ▼ to highlight **Secure browsing**, and then press **MENU/SELECT**.
2. On the **Secure browsing** menu, press **MENU/SELECT** to enable or disable HTTPS.



3. Press **ENTER** to save the setting.

Using the Provisioning menu

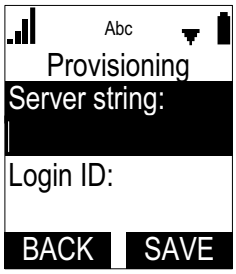
Use the Provisioning menu to configure auto-provisioning settings. For more information about auto-provisioning, see *"Provisioning" on page 63* and *"Provisioning Using Configuration Files" on page 73*.

On the Provisioning menu you can configure:

- Server string—the URL of the provisioning server. The URL can include a complete path to the configuration file.
- Login ID—the username the VSP600 will use to access the provisioning server.
- Login PW—the password the VSP600 will use to access the provisioning server.

To use the Provisioning menu:

1. From the **Admin Settings** menu, press ▼ to highlight **Provisioning**, and then press **SELECT**.
   The **Provisioning** menu appears.



2. Enter the server URL using the dial pad keys:
   - **BACKSP**—deletes a character
   - Press **1**, **0** and **#** to enter symbols. The period and "@" symbols are available under the **0** key.

   The format of the URL must be RFC 1738 compliant, as follows:
   "<schema>://<user>:<password>@<host>:<port>/<url-path>"

   "<user>:<password>@" may be empty.

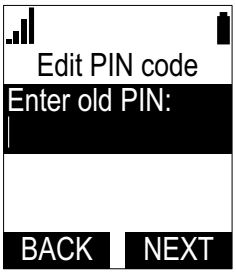
   "<port>" can be omitted if you do not need to specify the port number.
3. Press ▼ to move to the next line and enter the Login ID for access to the provisioning server if it is not part of the server string.
4. Press ▼ to move to the next line and enter the Login password.
5. Press **SAVE**.

Editing the handset PIN code

The PIN code is a four-digit code that you use to deregister the handset from the base. The default PIN is **1592**. Changing the PIN on the handset will change the PIN for all registered handsets.

To edit the PIN code:

1. From the Admin Settings menu, press ▼ to highlight **Edit PIN code**, and then press **SELECT**.
   The **Edit PIN code** screen appears.



2. Enter the current PIN using the dial pad keys.
3. Press **NEXT**.
4. Enter the new PIN and then press **NEXT**.
5. Confirm the new PIN and then press **SAVE**.

CHAPTER 3

USING THE WEBUI

The WebUI allows you to configure all aspects of VSP600 base station operation, including account settings, network settings, contact lists, and provisioning settings. The WebUI is embedded in the VSP600 operating system. When you access the WebUI, you are accessing it on the device, not on the Internet.

This chapter describes how to access the WebUI and configure VSP600 settings. This chapter covers:

Using the Web User Interface (WebUI)

The Web User Interface (WebUI) resides on the VSP600 base station. You can access it using an Internet browser. After you log in to the WebUI, you can configure the VSP600 on the following pages:

System

- SIP Account Management (see *page 30*)
- Call Settings (see *page 39*)
- User Preferences (see *page 41*)
- Signaling Settings (see *page 42*)
- Handset Settings (see *page 43*)

Network

- Basic Network Settings (see *page 45*)
- Advanced Network Settings (see *page 46*)

Contacts

- Base Directory (see *page 48*)
- Blacklist
- LDAP (see *page 54*)

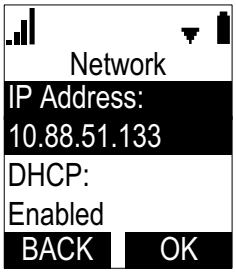
Servicing

- Reboot (see *page 57*)
- Time and Date (see *page 57*)
- Firmware Upgrade (see *page 60*)
- Provisioning (see *page 63*)
- Security (see *page 69*)
- Certificates (see *page 70*)
- System Logs (see *page 71*)

The WebUI also has a **System Status** and a **Handset Status** page, where you can view network status and general information about the VSP600 and handsets. The information on the Status page matches the **Status** menu available on the VSP601 handset.

To access the WebUI:

1. Ensure that your computer is connected to the same network as the VSP600.
2. Find the IP address of the VSP600:
   a. On a handset, press **MENU**.
   b. Press ▼ to highlight **Status**, and then press **ENTER**.
   c. With **Network** highlighted, press **ENTER**.
   The **Network** status screen appears.
   d. On the **Network** status screen, note the IP Address.



3. On your computer, open an Internet browser. (Depending on your browser, some of the pages presented here may look different and have different controls. Ensure that you are running the latest update of your preferred browser.)
4. Type the VSP600 IP address in the browser address bar and press **ENTER** on your computer keyboard.
   The browser displays a window asking for your user name and password.
5. For the user name, enter **admin**. For the password, enter the default password, **admin**. You can change the password later on the WebUI **Security** page, available under **Servicing**.
6. Click **OK**.
   The WebUI appears.

Click topics from the navigation bar along the top of the WebUI, and then click the links along the left to view individual pages. For your security, the WebUI times out after 10 minutes, so if it is idle for that time, you must log in again.

Most WebUI configuration pages have a Save button. Click Save to save changes you have made on the page. During a configuration session, click Save before you move on to the next WebUI page.

The remaining procedures in this section assume that you are already logged into the WebUI.

NOTE The settings tables in this section contain settings that appear in the WebUI and their equivalent settings in the configuration file template. You can use the configuration file template to create custom configuration files. Configuration files can be hosted on a provisioning server and used for automatically configuring phones. For more information, see *"Provisioning Using Configuration Files" on page 73*.

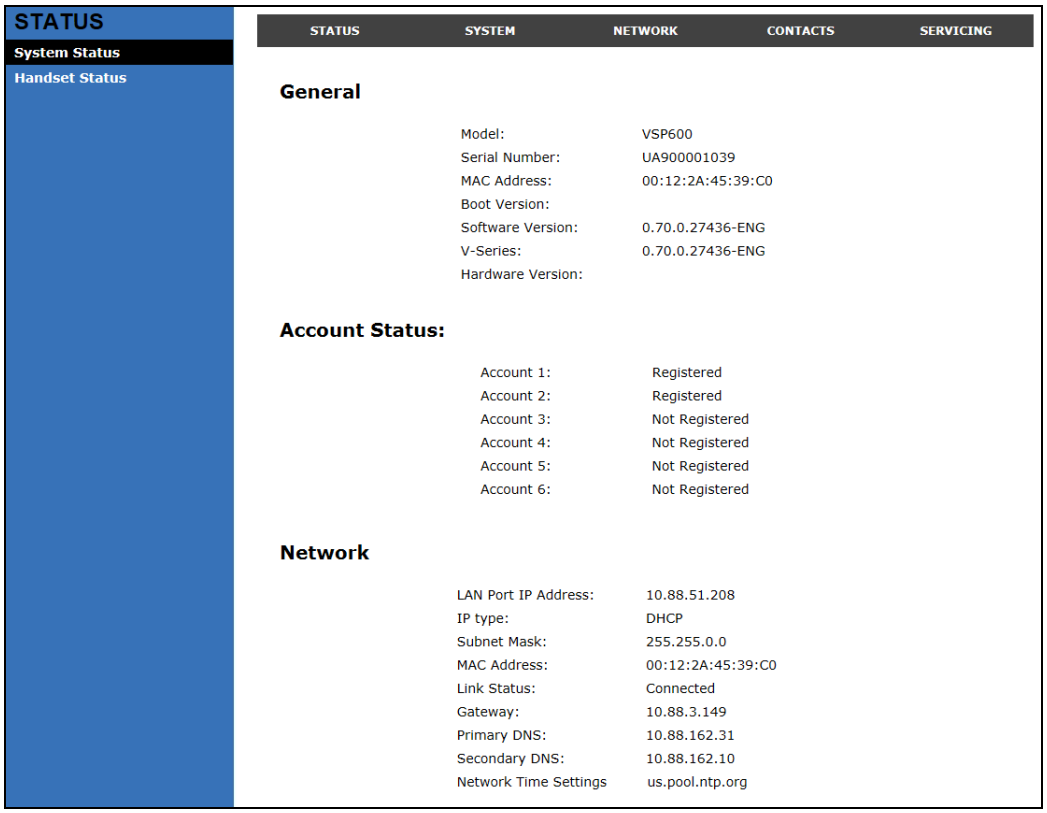
Status Page

On the Status pages, you can view network status and general information about the base station and handsets. Some of the information on the Status pages is also available on the Status menu available on the handset.

System Status

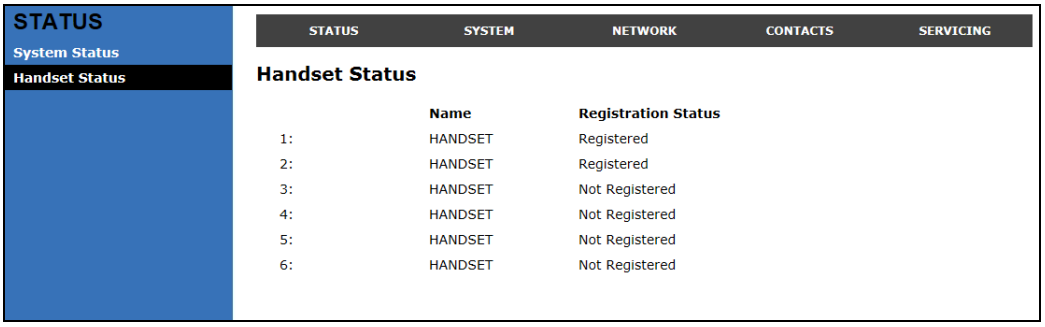
The System Status page shows:

- **General** information about your device, including model, MAC address, and firmware version
- **Account Status** information about your SIP account registration
- **Network** information regarding your device's network address and network connection



Handset Status

The handset status page shows the name and registration status of cordless handsets. The page lists the maximum of six handsets, even if fewer handsets are registered. If you have not given the handsets unique names, the default name of “HANDSET” appears.

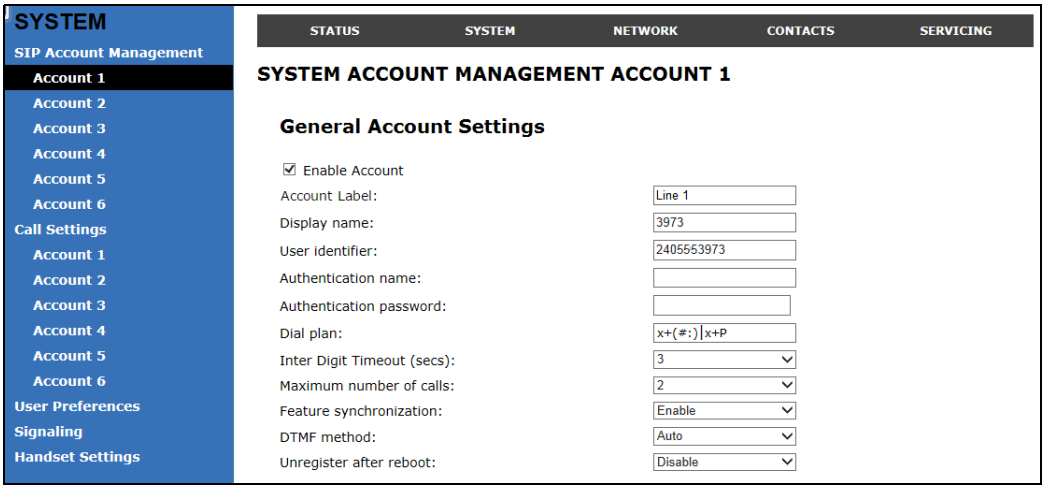


System Pages

SIP Account Management

On the SIP Account Management pages, you can configure each account you have ordered from your service provider.

The SIP Account settings are also available as parameters in the configuration file. See *"'sip_account" Module: SIP Account Settings" on page 82*.



General Account Settings

Click the link for each setting to see the matching configuration file parameter in *"Configuration File Parameter Guide" on page 81*. Default values and ranges are listed there.

Setting	Description
Enable Account	Enable or disable the SIP account. Select to enable.
Account Label	Enter the name that will appear on the VSP601 display when account x is selected. The Account Label identifies the SIP account throughout the WebUI and on the handset Dialing Line menu.
Display Name	Enter the Display Name. The Display Name is the text portion of the caller ID that is displayed for outgoing calls using account x.
User identifier	Enter the User identifier supplied by your service provider. The User ID, also known as the Account ID, is a SIP URI field used for SIP registration. **Note**: Do not enter the host name (e.g. "@sipservice.com"). The WebUI automatically adds the default host name.

Setting	Description
Authentication name	If authentication is enabled on the server, enter the authentication name (or authentication ID) for authentication with the server.
Authentication password	If authentication is enabled on the server, enter the authentication password for authentication with the server.
Dial Plan	Enter the dial plan, with dialing strings separated by a | symbol. See *"Dial Plan" on page 32*.
Inter Digit Timeout (secs)	Sets how long the VSP601 waits after any "P" (pause) in the dial string or in the dial plan.
Maximum Number of Calls	Select the maximum number of concurrent active calls allowed for that account.
Feature Synchronization	Enables the VSP600 to synchronize with Broadworks Application Server. Changes to features such as DND, Call Forward All, Call Forward No Answer, and Call Forward Busy on the server side will also update the settings on the VSP601 menu and WebUI. Similarly, changes made using the VSP601 or WebUI will update the settings on the server.
DTMF method	Select the default DTMF transmission method. You may need to adjust this if call quality problems are triggering unwanted DTMF tones or you have problems sending DTMF tones in general.
Unregister after reboot	Enables the phone to unregister the account(s) after rebooting-before the account(s) register again as the phone starts up. If other phones that share the same account(s) unregister unexpectedly in tandem with the rebooting VSP600, disable this setting.

Dial Plan

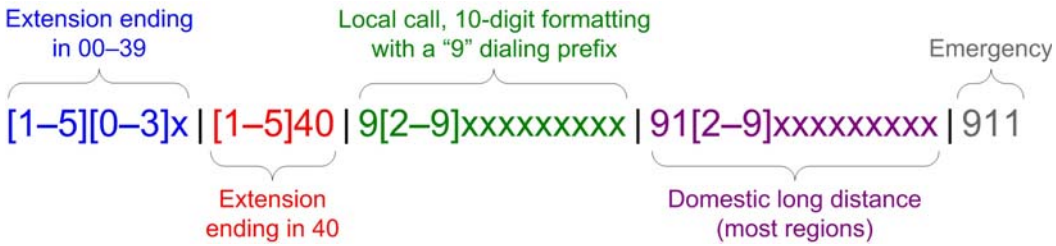
The dial plan consists of a series of dialing rules, or strings, that determine whether what the user has dialed is valid and when the VSP601 should dial the number.

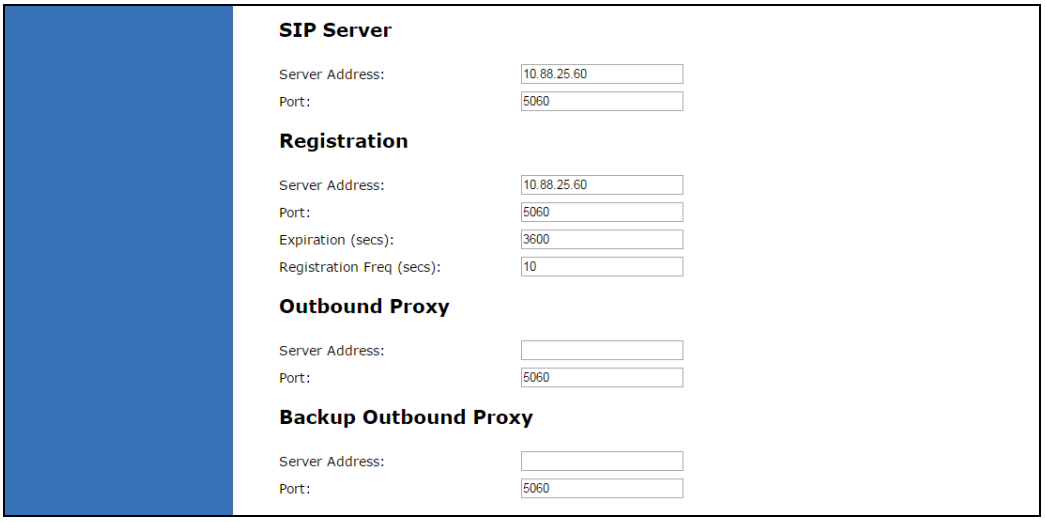
NOTE Numbers that are dialed when forwarding a call—when the user manually fowards a call, or a pre-configured number is dialed for Call Forward All, Call Forward–No Answer, or Call Forward Busy—always bypass the dial plan.

Dialing rules must consist of the elements defined in the table below.

Element	Description
x	Any dial pad key from 0 to 9, including # and *.
[0-9]	Any two numbers separated by a hyphen, where the second number is greater than the first. All numbers within the range or valid, excluding # and *.
x+	An unlimited series of digits.
,	This represents the playing of a secondary dial tone after the user enters the digit(s) specified or dials an external call prefix before the comma. For instance, "9,xxxxxxx" means the secondary dial tone is played after the user dials 9 until any new digit is entered. "9,3xxxxxx" means only when the digit 3 is hit would the secondary dial tone stop playing.
PX	This represents a pause of a defined time; X is the pause duration in seconds. For instance, "P3" would represent pause duration of 3 seconds. When "P" only is used, the pause time is the same as the Inter Digit Timeout (see *"SIP Account Management" on page 30*).
(0:9)	This is a substitution rule where the first number is replaced by the second. For example, "(4:723)xxxx" would replace "46789" with "723-6789". If the substituted number (the first number) is empty, the second number is added to the number dialed. For example, in "(:1)xxxxxxxxxx", the digit 1 is appended to any 10-digit number dialed.
|	This separator is used to indicate the start of a new pattern. Can be used to add multiple dialing rules to one pattern edit box.

A sample dial plan appears below.





SIP Server Settings

Setting	Description
Server address	Enter the IP address or domain name for the SIP server.
Server port	Enter the port number that the SIP server will use.

Registration Settings

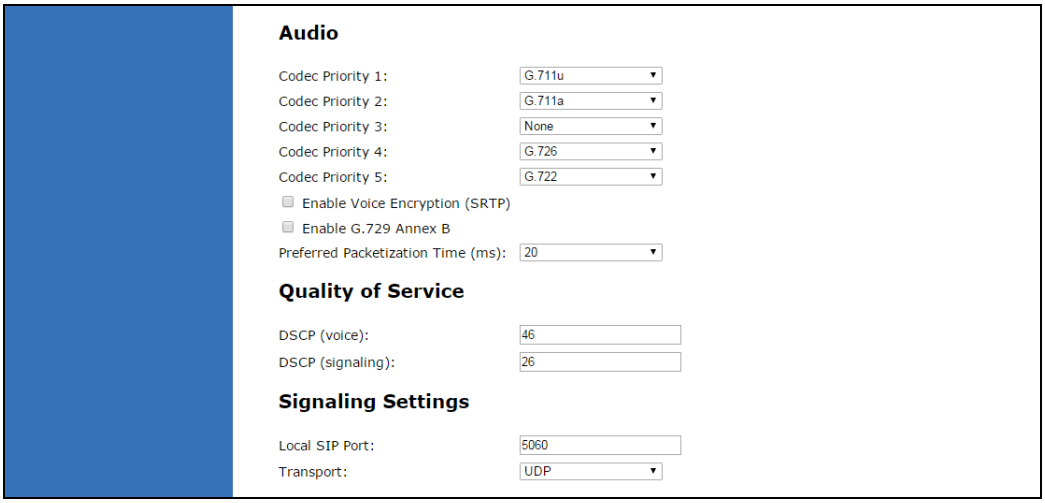
Setting	Description
Server address	Enter the IP address or domain name for the registrar server.
Server port	Enter the port number that the registrar server will use.
Expiration	Enter the desired registration expiry time in seconds.
Registration Freq (secs)	Enter the desired registration retry frequency in seconds. If registration using the Primary Outbound Proxy fails, the Registration Freq setting determines the number of seconds before a registration attempt is made using the Backup Outbound Proxy.

Outbound Proxy Settings

Setting	Description
Server address	Enter the IP address or domain name for the proxy server.
Server port	Enter the port number that the proxy server will use.

Backup Outbound Proxy Settings

Setting	Description
Server address	Enter the IP address or domain name for the backup proxy server.
Server port	Enter the port number that the backup proxy server will use.



Audio Settings

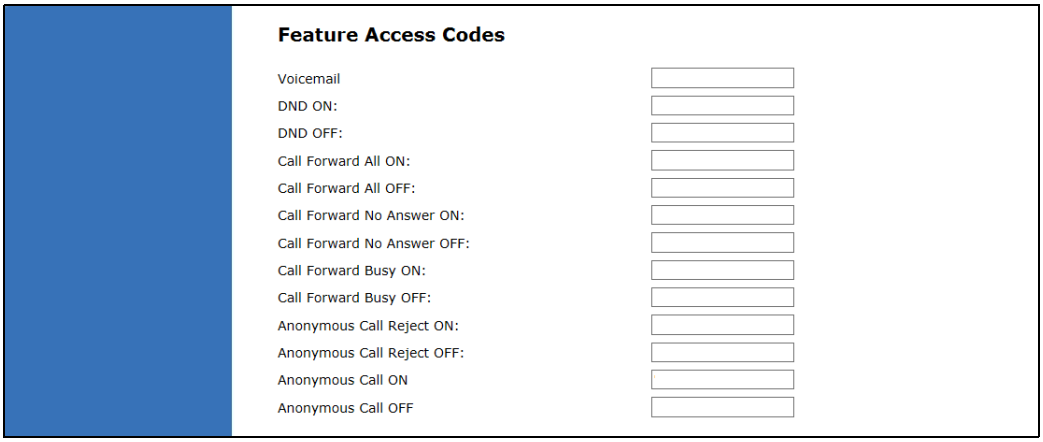
Setting	Description
Codec priority 1	Select the codec to be used first during a call.
Codec priority 2	Select the codec to be used second during a call if the previous codec fails.
Codec priority 3	Select the codec to be used third during a call if the previous codec fails.
Codec priority 4	Select the codec to be used fourth during a call if the previous codec fails.
Codec priority 5	Select the codec to be used fifth during a call if the previous codec fails.
Enable voice encryption (SRTP)	Select to enable secure RTP for voice packets.
Enable G.729 Annex B	When G.729a/b is enabled, select to enable G.729 Annex B, with voice activity detection (VAD) and bandwidth-conserving silence suppression.
Preferred Packetization Time (ms)	Select the packetization interval time.

Quality of Service

Setting	Description
DSCP (voice)	Enter the Differentiated Services Code Point (DSCP) value from the Quality of Service setting on your router or switch.
DSCP (signalling)	Enter the Differentiated Services Code Point (DSCP) value from the Quality of Service setting on your router or switch.

Signaling Settings

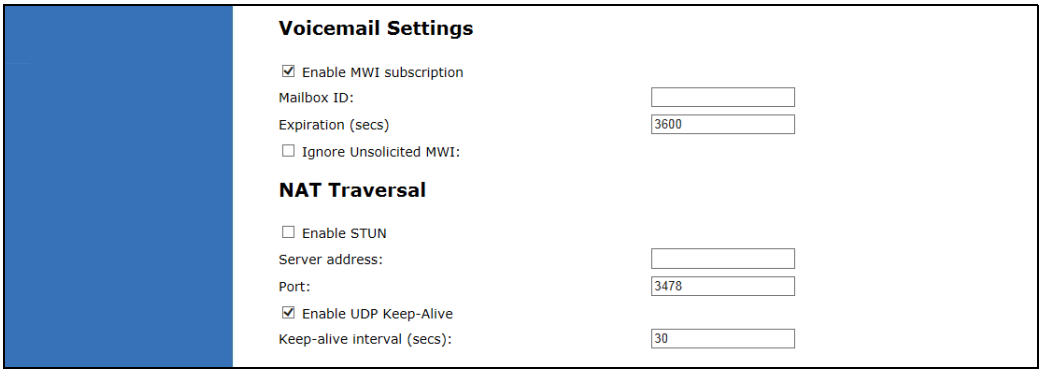
Setting	Description
Local SIP port	Enter the local SIP port.
Transport	Select the SIP transport protocol: ■ TCP (Transmission Control Protocol) is the most reliable protocol and includes error checking and delivery validation. ■ UDP (User Datagram Protocol) is generally less prone to latency, but SIP data may be subject to network congestion. ■ TLS (Transport Layer Security)—the VSP600 supports secured SIP signalling via TLS. Optional server authentication is supported via user-uploaded certificates. TLS certificates are uploaded using the configuration file. See *""file" Module: Imported File Settings" on page 116* and consult your service provider.



Feature Access Codes Settings

If your IP PBX service provider uses feature access codes, then enter the applicable codes here.

Setting	Description
Voicemail	Enter the voicemail access code. The code is dialed when the user selects a line from the Message menu.
DND ON	Enter the Do Not Disturb ON access code.
DND OFF	Enter the Do Not Disturb OFF access code.
Call Forward All ON	Enter the Call Forward All ON access code.
Call Forward All OFF	Enter the Call Forward All OFF access code.
Call Forward No Answer ON	Enter the Call Forward No Answer ON access code.
Call Forward No Answer OFF	Enter the Call Forward No Answer OFF access code.
Call Forward Busy ON	Enter the Call Forward Busy ON access code.
Call Forward Busy OFF	Enter the Call Forward Busy OFF access code.
Anonymous Call Reject ON	Enter the Anonymous Call Reject ON access code.
Anonymous Call Reject OFF	Enter the Anonymous Call Reject OFF access code.
Anonymous Call ON	Enter the Anonymous Call ON access code.
Anonymous Call OFF	Enter the Anonymous Call OFF access code.

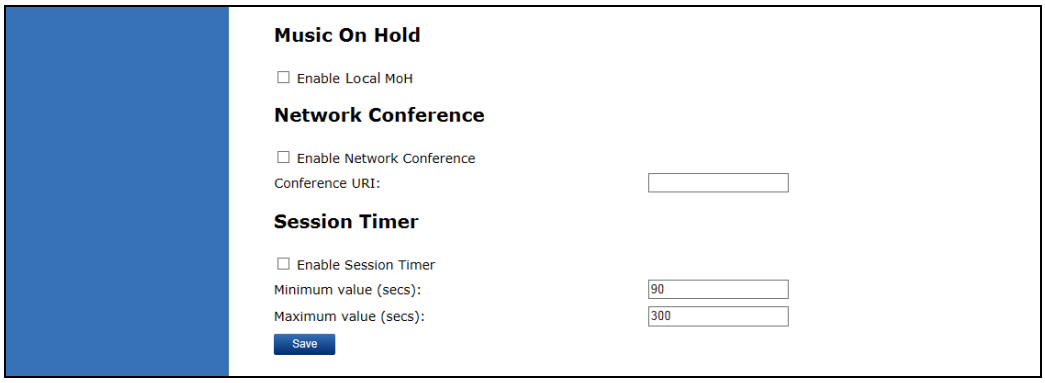


Voicemail Settings

Setting	Description
Enable MWI Subscription	When enabled, the account subscribes to the "message summary" event package. The account may use the User ID or the service provider's "Mailbox ID".
Mailbox ID	Enter the URI for the mailbox ID. The phone uses this URI for the MWI subscription. If left blank, the User ID is used for the MWI subscription.
MWI subscription expiration	Enter the MWI subscription expiry time (in seconds) for account x.
Ignore unsolicited MWI	When selected, unsolicited MWI notifications—notifications in addition to, or instead of SUBSCRIBE and NOTIFY methods—are ignored for account x. If the VSP600 receives unsolicited MWI notifications, the Message Waiting LED will not light to indicate new messages. Disable this setting if: ■ MWI service does not involve a subscription to a voicemail server. That is, the server supports unsolicited MWI notifications. ■ you want the Message Waiting LED to indicate new messages when the VSP600 receives unsolicited MWI notifications.

NAT Traversal

Setting	Description
Enable STUN	Enables or disables STUN (Simple Traversal of UDP through NATs) for account x. The Enable STUN setting allows the VSP600 to identify its publicly addressable information behind a NAT via communicating with a STUN server.
Server address	Enter the STUN server IP address or domain name.
Server port	Enter the STUN server port.
Enable UDP Keep-Alive	Enables or disables UDP keep-alives. Keep-alive packets are used to maintain connections established through NAT.
Keep-alive interval (secs)	Enter the interval (in seconds) for sending UDP keep-alives.



Music on Hold Settings

Setting	Description
Enable Local MoH	Enables or disables a hold-reminder tone that the user hears when a far-end caller puts the call on hold.

Network Conference Settings

Setting	Description
Enable Network Conference	Enables or disables network conferencing for account x.
Conference URI	Enter the URI for the network bridge for conference handling on account x.

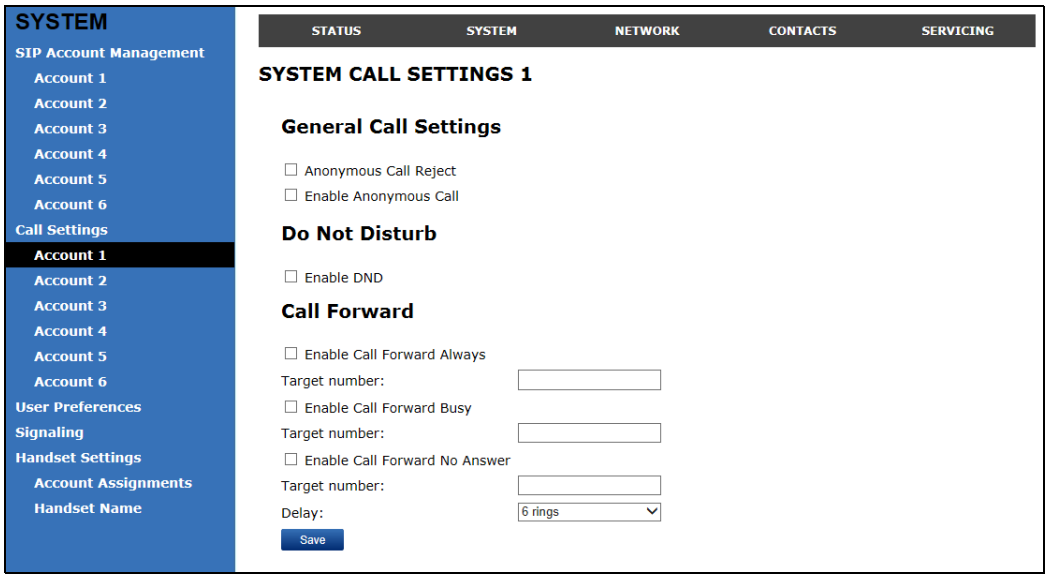
Session Timer

Setting	Description
Enable Session Timer	Enables or disables the SIP session timer. The session timer allows a periodic refreshing of a SIP session using the RE-INVITE message.
Minimum value (secs)	Sets the session timer minimum value (in seconds) for account x.
Maximum value (secs)	Sets the session timer maximum value (in seconds) for account x.

Call Settings

You can configure call settings for each account. Call Settings include Do Not Disturb and Call Forward settings.

The call settings are also available as parameters in the configuration file. See *""call_settings" Module: Call Settings" on page 114*.



General Call Settings

Setting	Description
Anonymous Call Reject	Enables or disables rejecting calls indicated as "Anonymous."
Enable Anonymous Call	Enables or disables outgoing anonymous calls. When enabled, the caller name and number are indicated as "Anonymous."

Do Not Disturb

Setting	Description
Enable DND	Turns Do Not Disturb on or off.

Call Forward

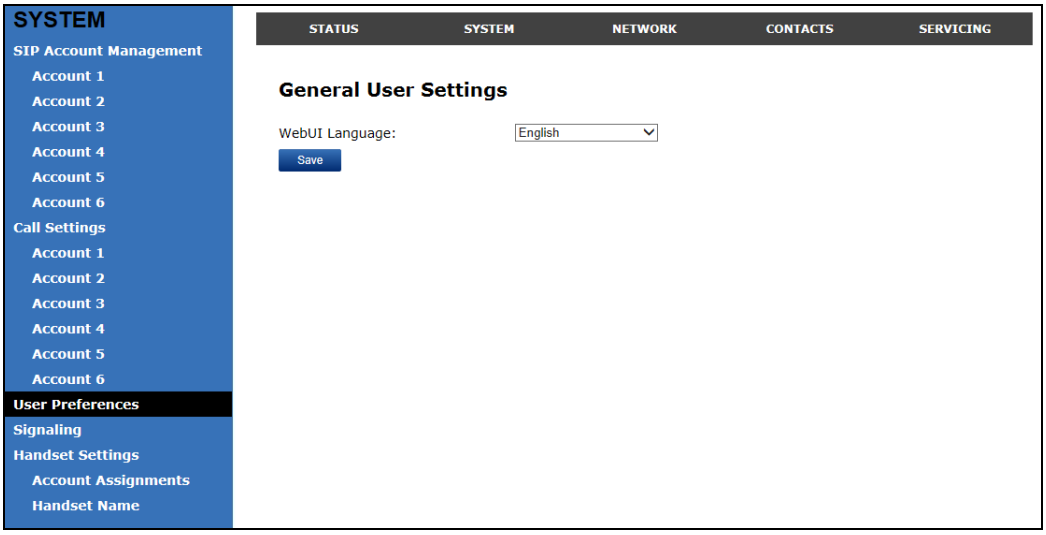
Setting	Description
Enable Call Forward Always	Enables or disables call forwarding for all calls on that line. Select to enable.
Target Number	Enter a number to which all calls will be forwarded.

Setting	Description
Enable Call Forward Busy	Enables or disables forwarding incoming calls to the target number if: ■ the number of active calls has reached the maximum number of calls configured for account x ■ Call Waiting Off is selected.
Target Number	Enter a number to which calls will be forwarded when Call Forward Busy is enabled.
Enable Call Forward No Answer	Enables or disables call forwarding for unanswered calls on that line.
Target Number	Enter a number to which unanswered calls will be forwarded.
Delay	Select the number of rings before unanswered calls are forwarded.

Preferences

On the Preferences page, you can set the language that appears on the WebUI. The Preferences page is also available to phone users when they log on to the WebUI.

The preference settings are also available as parameters in the configuration file. See *""user_pref" Module: User Preference Settings" on page 113*.



General User Settings

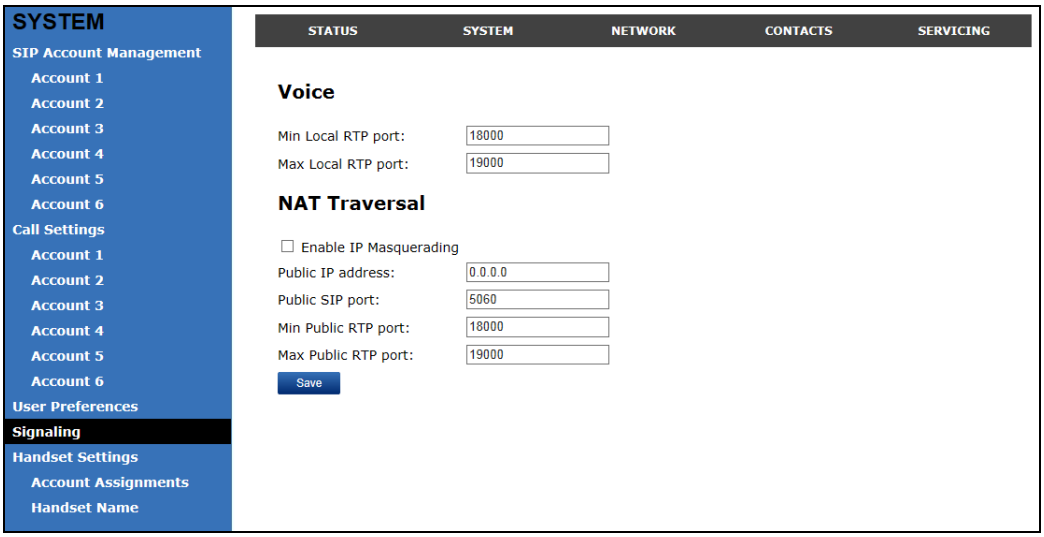
Click the link for each setting to see the matching configuration file parameter in *"Configuration File Parameter Guide" on page 81*. Default values and ranges are listed there.

Setting	Description
WebUI Language	Sets the language that appears on the WebUI.

Signaling Settings

The signaling settings are also available as parameters in the configuration file. See *""network" Module: Network Settings" on page 94*.

After entering information on this page, click Save to save it.



Voice

Click the link for each setting to see the matching configuration file parameter in *""network" Module: Network Settings" on page 94*. Default values and ranges are listed there.

Setting	Description
Min Local RTP port	Enter the lower limit of the Real-time Transport Protocol (RTP) port range. RTP ports specify the minimum and maximum port values that the phone will use for RTP packets.
Max Local RTP port	Enter the upper limit of the RTP port range.

NAT Traversal

The NAT Traversal settings are communicated to the VoIP server so that the VSP600 is reachable when connected to the Internet behind NAT.

Setting	Description
Enable IP Masquerading	Select to enable NAT traversal and IP masquerading.
Public IP address	Enter the external IP address of your router. This setting identifies the router's public address to the VoIP server.
Public SIP port	Enter the router port number being used for SIP. This setting identifies the router's port to the VoIP server.
Min Public RTP port	Enter the lower limit of the public RTP port range.

Setting	Description
Max Public RTP port	Enter the upper limit of the RTP port range.

Handset Settings

The Handset Settings allow you to configure account assignments and names for the cordless handsets that are registered to the base station. For more information on registering cordless handsets, see the VSP600/VSP601 User Guide.

The network settings are also available as parameters in the configuration file. See *“"hs_settings" Module: Handset Settings” on page 93*.

Account Assignments

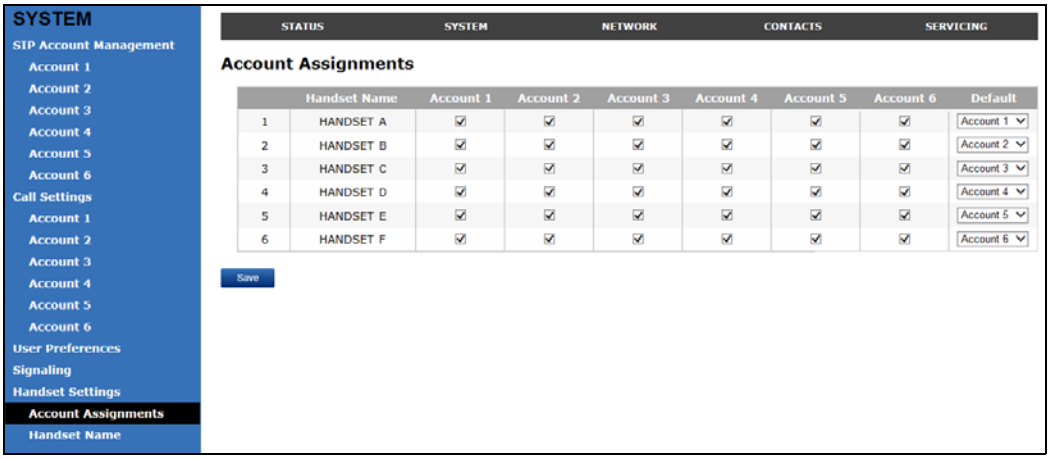
The **Account Assignments** table lists the maximum of six handsets, even if there a fewer handsets registered. The registration status of currently registered handsets does not affect what is listed on this table.

The table always displays the maximum six accounts, even if there are fewer SIP accounts enabled.

If you have not entered any unique handset names yet, then the default name of "HANDSET" appears.

On the Account Assignments table, you can select which accounts will be available for both incoming and outgoing calls on each handset.

The handset will first attempt to use the account you select under Default when going off-hook.

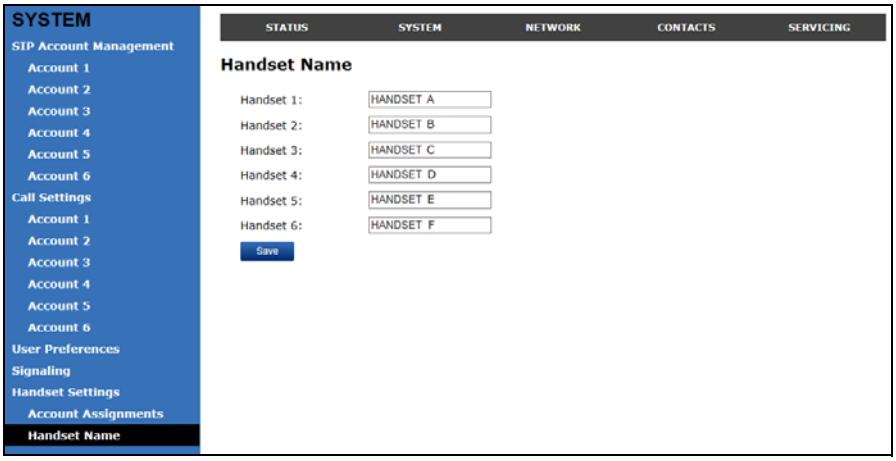


Handset Name

On the **Handset Name** page, you can enter a name for each Handset. The Handset Name will be used throughout the WebUI and will appear on the handset Idle screen.

The Handset Name is limited to a maximum of 11 characters.

The default name is "HANDSET". Blank name fields are not allowed. If you click Save when any fields are empty, an error message appears.



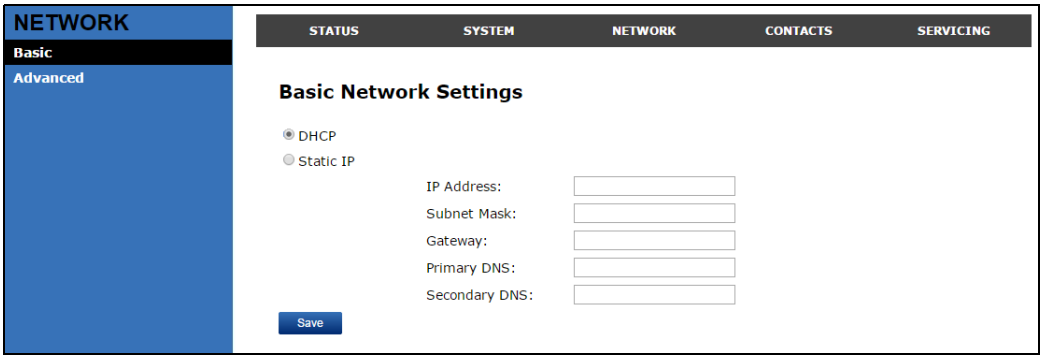
Network Pages

You can set up the VSP600 for your network configuration on the Network pages. Your service provider may require you to configure your network to be compatible with its service, and the VSP600 settings must match the network settings.

The network settings are also available as parameters in the configuration file. See *""network" Module: Network Settings" on page 94*.

After entering information on this page, click Save to save it.

Basic Network Settings



NOTE If you disable DHCP on this page, you must configure static IP settings for the VSP600. You must be familiar with TCP/IP principles and protocols to configure static IP settings.

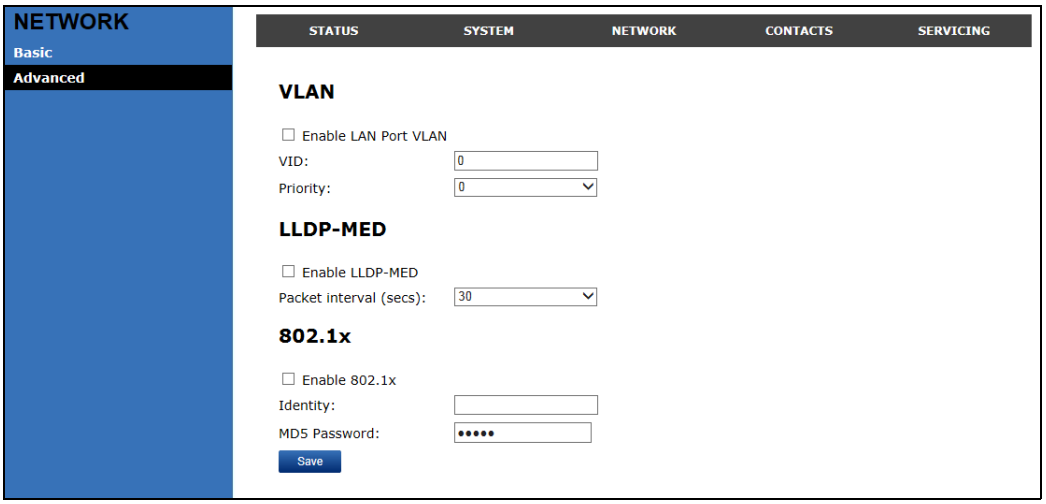
Basic Network Settings

Click the link for each setting to see the matching configuration file parameter in *""network" Module: Network Settings" on page 94*. Default values and ranges are listed there.

Setting	Description
DHCP	DHCP is selected (enabled) by default, which means the VSP600 will get its IP address, Subnet Mask, Gateway, and DNS Server(s) from the network. When DHCP is disabled, you must enter a static IP address for the VSP600, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).
Static IP	When Static IP is selected, you must enter a static IP address for the VSP600, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).
IP Address	If DHCP is disabled, enter a static IP address for the VSP600.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the address of the default gateway (in this case, your router).

Setting	Description
Primary DNS	If DHCP is disabled, enter addresses for the primary and secondary DNS servers.
Secondary DNS	

Advanced Network Settings



VLAN

You can organize your network and optimize VoIP performance by creating a virtual LAN for phones and related devices.

Click the link for each setting to see the matching configuration file parameter in *""network" Module: Network Settings" on page 94*. Default values and ranges are listed there.

Setting	Description
Enable LAN Port VLAN	Enable if the phone is part of a VLAN on your network. Select to enable.
VID	Enter the VLAN ID (vlan 5, for example).
Priority	Select the VLAN priority that matches the Quality of Service (QOS) settings that you have set for that VLAN ID. Outbound SIP packets will be marked and sent according to their priority. 7 is the highest priority. **Note**: Configuring QOS settings for your router or switch is a subject outside the scope of this document.

LLDP-MED

Setting	Description
Enable LLDP-MED	Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). LLDP-MED is a standards-based discovery protocol supported on some network switches. It is required for auto-configuration with VLAN settings.
Packet Interval (secs)	Sets the LLDP-MED packet interval (in seconds).

802.1x

Setting	Description
Enable 802.1x	Enables or disables the 802.1x authentication protocol. This protocol allows the phone to attach itself to network equipment that requires device authentication via 802.1x.
Identity	Enter the 802.1x EAPOL identity.
MD5 Password	Enter the 802.1x EAPOL MD5 password.

Contacts Pages

Base Directory

On the Base Directory page, you can manage directory entries that will be available on all handsets. You can sort, edit, delete, and add contact information for up to 200 entries. In order to back up your contacts or import another local directory file, the page also enables you to export and import the base directory.

The Base Directory lists entries on up to 10 pages, with 20 entries per page. Click Next, Last, First, or a page number to view the desired page of entries.

NOTE Each handset also has its own directory. You can add entries to the handset directory using the handset. For more information, see the VSP600/VSP601 User Guide.

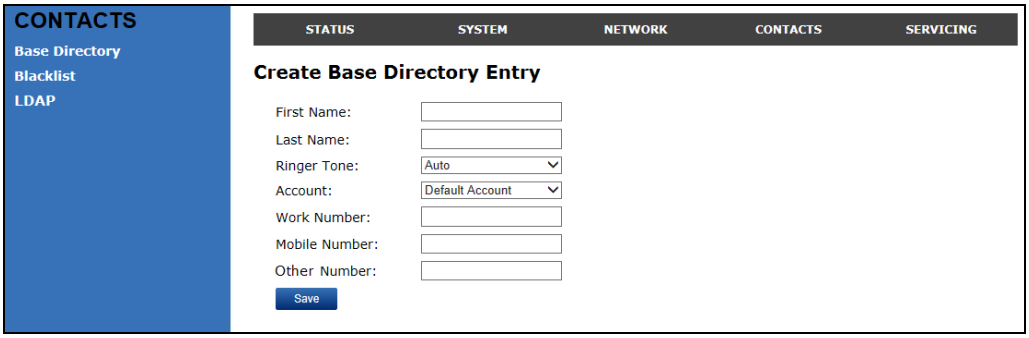
Table 5 describes the buttons available on the Base Directory page.

Table 5. Base Directory commands

Click	To...
Sort By Last Name	Sort the list by last name.
Edit	Edit information for an entry
Next	View the next page of entries.
Last	View the last page of entries.
First	View the first page of entries.
Delete Selected Entries	Delete selected entries from the directory. Click **Select All** to select every entry on the page you are viewing.
Add New Entry	Add a new directory entry.
Clear Directory	Delete all Directory entries.
Choose File	Import a directory file.
Export	Export the directory.

To add a new directory entry:

1. Click Add New Entry .
   The **Create Base Directory Entry** page appears.



2. Enter the required information as described in the following table.

Create Base Directory Entry

Setting	Description	Range	Default
First Name	Enter the appropriate names in these fields. The maximum length of the first name and last name fields is 15 characters.	n/a	Blank
Last Name			
Ringer Tone	Sets a unique ringer tone for calls from this directory entry.	Auto, Tone 1–10	Tone 1
Account	Sets the account used when you dial this directory entry.	Default Account, Account 1–6	Default Account
Work Number	Enter the appropriate names and numbers in these fields.	n/a	Blank
Mobile Number			
Other Number			

Directory Import/Export

The best way to create a directory file for import is to first export the directory from the phone. After exporting the file, open it in an .xml editor and add or modify entries.

Importing a directory file adds the imported directory entries to existing entries. Therefore, it is possible to have duplicate entries after importing a directory file. If you are importing a "complete" directory file with the aim of replacing the entire current directory, use **Select All** and Delete Selected Entries to clear the directory before importing the file.

NOTE Using the configuration file, you can set whether an imported directory file adds to existing entries or replaces existing entries. See *""file" Module: Imported File Settings" on page 116*.

Directory files are .xml files that have the following tags:

Local Directory WebUI field	Directory file XML tag
First Name	<DIR_ENTRY_NAME_FIRST>
Last Name	<DIR_ENTRY_NAME_LAST>
Work Number	<DIR_ENTRY_NUMBER_WORK>
Mobile Number	<DIR_ENTRY_NUMBER_MOBILE>
Other Number	<DIR_ENTRY_NUMBER_OTHER>
Account	<DIR_ENTRY_LINE_NUMBER>
Call Block (not on WebUI)	<DIR_ENTRY_BLOCK>
Ringer Tone	<DIR_ENTRY_RINGER>

Blacklist

On the Blacklist page, you can manage local blacklist entries. The VSP600 rejects calls from numbers that match blacklist entries. You can sort, edit, delete, and add up to 200 blacklist entries. In order to back up your blacklist entries or import another local blacklist file, the page also enables you to export and import the blacklist.

The blacklist lists entries on up to 10 pages, with 20 entries per page. Click Next, Last, First, or a page number to view the desired page of entries.

NOTE You can also use the VSP601 menu to manage blacklist entries. For more information, see the VSP600/VSP601 User Guide.

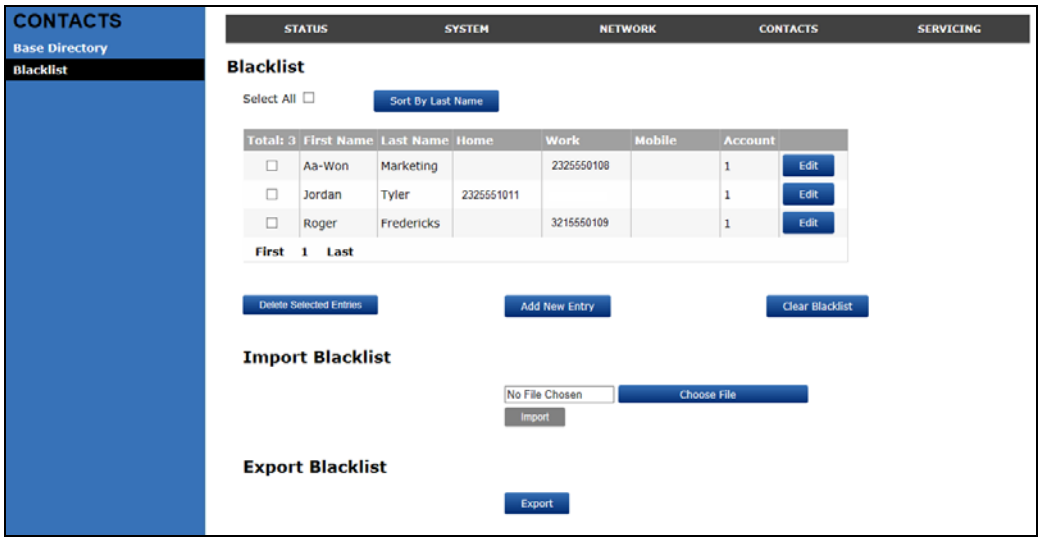


Table 6 describes the buttons available on the Blacklist page.

Table 6. Blacklist commands

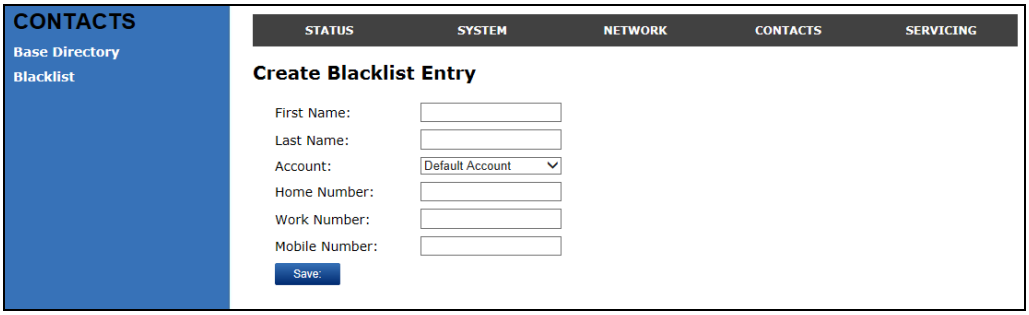
Click	To...
Sort By Last Name	Sort the list by last name.
Edit	Edit information for an entry
Next	View the next page of entries.
Last	View the last page of entries.
First	View the first page of entries.
Delete Selected Entries	Delete selected entries. Click **Select All** to select every entry on the page you are viewing.

Table 6. Blacklist commands

Click	To...
Add New Entry	Add a new entry.
Clear Directory	Delete all entries.
Choose File	Import a blacklist file.
Export	Export the blacklist.

To add a new blacklist entry:

1. Click Add New Entry .
   The **Create Blacklist Entry** page appears.



2. Enter the required information as described in the following table.

Create Blacklist Entry

Setting	Description	Range	Default
First Name	Enter the appropriate names in these fields. The maximum length of the first name and last name fields is 15 characters.	n/a	Blank
Last Name			
Account	Sets the account used when you dial this directory entry.	Default Account, Account 1–6	Account 1
Work Number	Enter the appropriate names and numbers in these fields.	n/a	Blank
Mobile Number			
Other Number			

Blacklist Import/Export

The best way to create a blacklist file for import is to first export the blacklist from the VSP600. After exporting the file, open it in an .xml editor and add or modify entries.

Importing a blacklist file adds the imported blacklist entries to existing entries. Therefore, it is possible to have duplicate entries after importing a blacklist file. If you are importing a "complete" blacklist file with the aim of replacing the entire current blacklist, use **Select All** and 

to clear the blacklist before importing the file.

NOTE Using the configuration file, you can set whether an imported blacklist file adds to or replaces existing entries. See *""file" Module: Imported File Settings" on page 116*.

Blacklist files are .xml files that have the following tags:

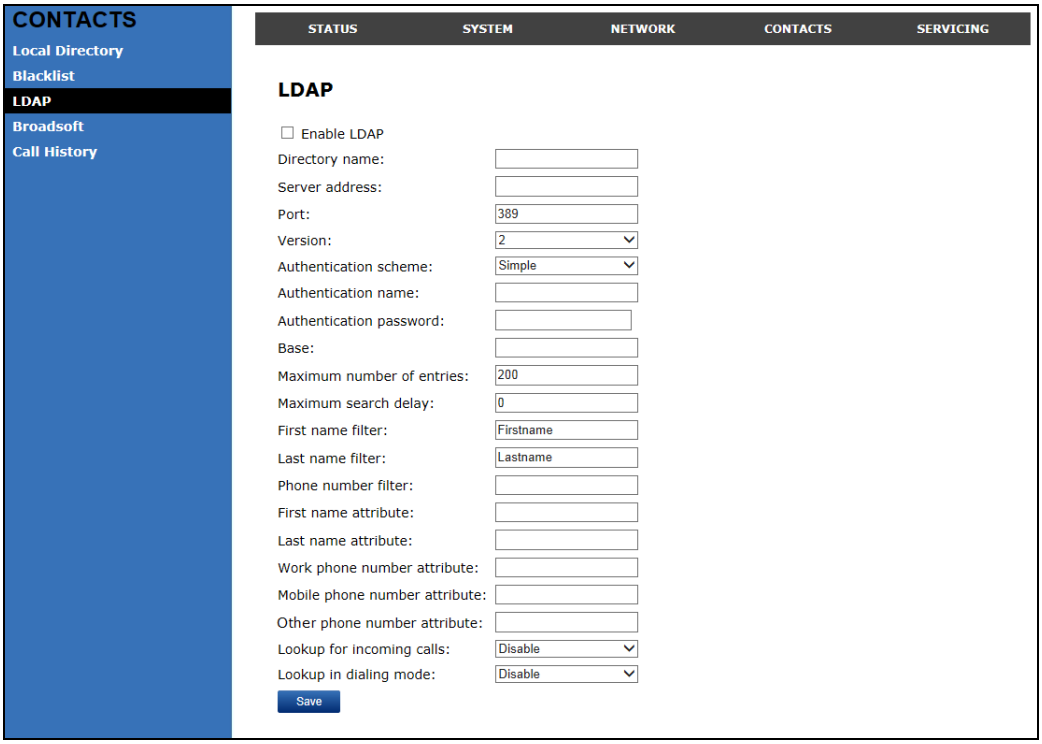
Blacklist WebUI field	Blacklist file XML tag
First Name	<BLACKLIST_ENTRY_NAME_FIRST>
Last Name	<BLACKLIST_ENTRY_NAME_LAST>
Work Number	<BLACKLIST_ENTRY_NUMBER_WORK>
Mobile Number	<BLACKLIST_ENTRY_NUMBER_MOBILE>
Other Number	<BLACKLIST_ENTRY_NUMBER_OTHER>
Account	<BLACKLIST_ENTRY_LINE_NUMBER>

LDAP

The phone supports remote Lightweight Directory Access Protocol (LDAP) directories. An LDAP directory is hosted on a remote server and may be the central directory for a large organization spread across several cities, offices, and departments. You can configure the phone to access the directory and allow users to search the directory for names and telephone numbers.

The LDAP settings are also available as parameters in the configuration file. See *“"remoteDir" Module: Remote Directory Settings” on page 108*.

After entering information on this page, click Save to save it.



LDAP Settings

Click the link for each setting to see the matching configuration file parameter in *“"remoteDir" Module: Remote Directory Settings” on page 108*. Default values and ranges are listed there.

Setting	Description
Enable LDAP	Enables or disables the phone's access to the LDAP directory.
Directory name	Enter the LDAP directory name.
Server address	Enter the LDAP server domain name or IP address.
Port	Enter the LDAP server port.

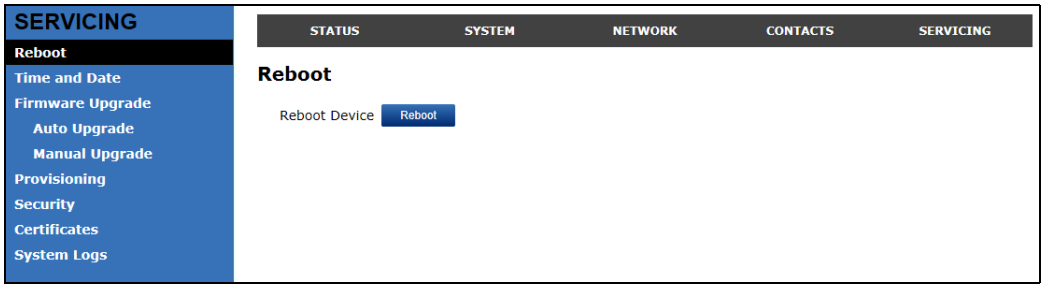
Setting	Description
Version	Select the LDAP protocol version supported on the phone. Ensure the protocol value matches the version assigned on the LDAP server.
Authentication scheme	Select the LDAP server authentication scheme.
Authentication name	Enter the user name or authentication name for LDAP server access.
Authentication password	Enter the authentication password for LDAP server access.
Base	Enter the LDAP search base. This sets where the search begins in the directory tree structure. Enter one of more attribute definitions, separated by commas (no spaces). Your directory may include attributes like "cn" (common name) or "ou" (organizational unit) or "dc" (domain component). For example: ou=accounting,dc=vtech,dc=com
Maximum number of entries	Sets the maximum number of entries returned for an LDAP search. Limiting the number of hits can conserve network bandwidth.
Maximum search delay	Enter the delay (in seconds) before the phone starts returning search results.
First name filter	Enter the first name attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
Last name filter	Enter the last name attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
Phone number filter	Enter the number attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
First name attribute	Sets the attribute for first name. What you enter here should match the first name attribute for entries on the LDAP server (gn for givenName, for example). This helps ensure that the phone displays LDAP entries in the same format as the Local Directory.
Last name attribute	Sets the attribute for last name. What you enter here should match the last name attribute for entries on the LDAP server (sn for surname, for example). This helps ensure that the phone displays LDAP entries in the same format as the Local Directory.

Setting	Description
Work number attribute	Sets the attribute for the work number. What you enter here should match the work number attribute for entries on the LDAP server (telephoneNumber, for example). This helps ensure that the phone displays LDAP entries in the same format as the Local Directory.
Mobile number attribute	Sets the attribute for the mobile number. What you enter here should match the mobile number attribute for entries on the LDAP server (mobile, for example). This helps ensure that the phone displays LDAP entries in the same format as the Local Directory.
Other number attribute	Sets the attribute for the other number. What you enter here should match the other number attribute for entries on the LDAP server (otherPhone, for example). This helps ensure that the phone displays LDAP entries in the same format as the Local Directory.
Lookup for incoming calls	Enables or disables LDAP incoming call lookup. If enabled, the phone searches the LDAP directory for the incoming call number. If the number is found, the phone uses the LDAP entry for CID info.
Lookup in dialing mode	Enables or disables LDAP outgoing call lookup. If enabled, numbers entered in pre-dial or live dial are matched against LDAP entries. If a match is found, the LDAP entry is displayed for dialing.

Servicing Pages

Reboot

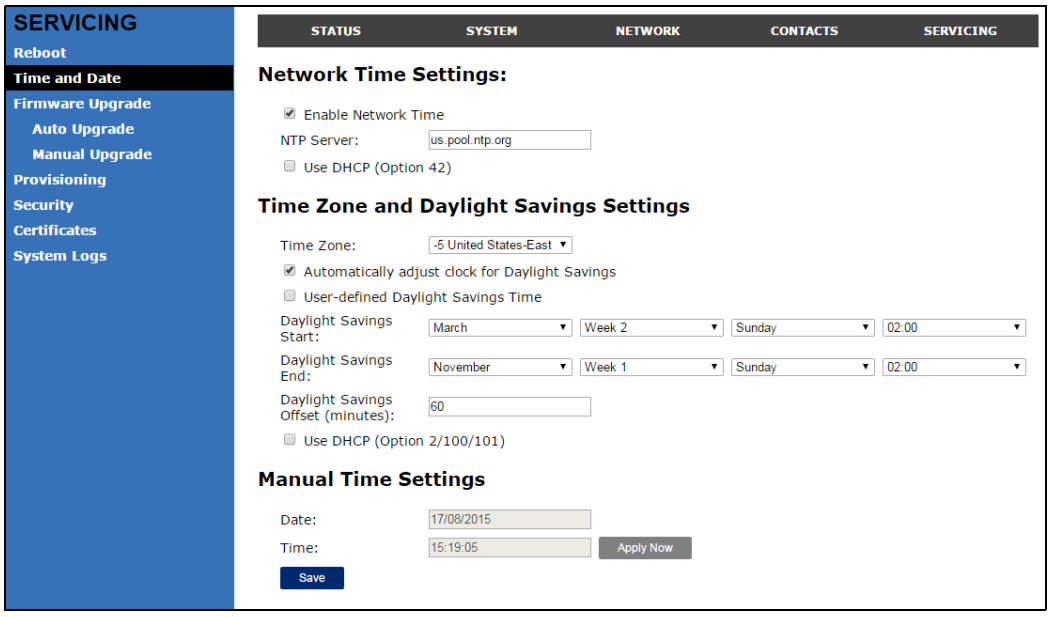
To manually reboot the VSP600 and apply settings that you have updated, click Reboot .



Time and Date

On the Time and Date page, you can manually set the time and date, and the time and date formats. You can also set the system time to follow a Network Time Protocol (NTP) Server (recommended) or you can set the time and date manually.

The time and date settings are also available as parameters in the configuration file. See *""time_date" Module: Time and Date Settings" on page 103*.



Network Time Settings

Setting	Description
Enable Network Time	Enables or disables getting time and date information for your phone from the Internet.

Setting	Description
NTP Server	If Enable Network Time is selected, enter the URL of your preferred time server.
Use DHCP (Option 42)	If Enable Network Time is selected, select to use DHCP to locate the time server. Option 42 specifies the NTP server available to the phone. When enabled, the phone obtains the time in the following priority: 1. Option 42 2. NTP Server 3. Manual time.

Time Zone and Daylight Savings Settings

Setting	Description
Time Zone	Select your time zone from the list.
Automatically adjust clock for Daylight Savings	Select to adjust the clock for daylight savings time according to the NTP server and time zone setting. To disable daylight savings adjustment, disable both this setting and User-defined Daylight Savings Time.
User-defined DST	Select to set your own start and end dates and offset for Daylight Savings Time. To disable daylight savings adjustment, disable both this setting and Automatically adjust clock for Daylight Savings.
DST Start: Month DST Start: Week DST Start: Day DST Start: Hour	If User-defined DST is enabled, set the start date and time for daylight savings: Month, week, day, and hour.
DST End: Month DST End: Week DST End: Day DST End: Hour	If User-defined DST is enabled, set the end date and time for daylight savings: Month, week, day, and hour.
Daylight Savings Offset	If User-defined DST is enabled, this specifies the daylight savings adjustment (in minutes) to be applied when the current time is between Daylight Savings Start and Daylight Savings End.
Use DHCP (Option 2/100/101)	If Enable Network Time is selected, select to use DHCP to determine the time zone offset. Options 2, 100 and 101 determine time zone information.

Manual Time Settings

If Enable Network Time is disabled or if the time server is not available, use Manual Time Settings to set the current time.

Setting	Description
Date	Select the current year, month, and day. Click the **Date** field and select the date from the calendar that appears.
Time	Sets the current hour, minute, and second. Click the Time field, and enter the current time. You can also refresh the page to update the manual time settings.

Click 

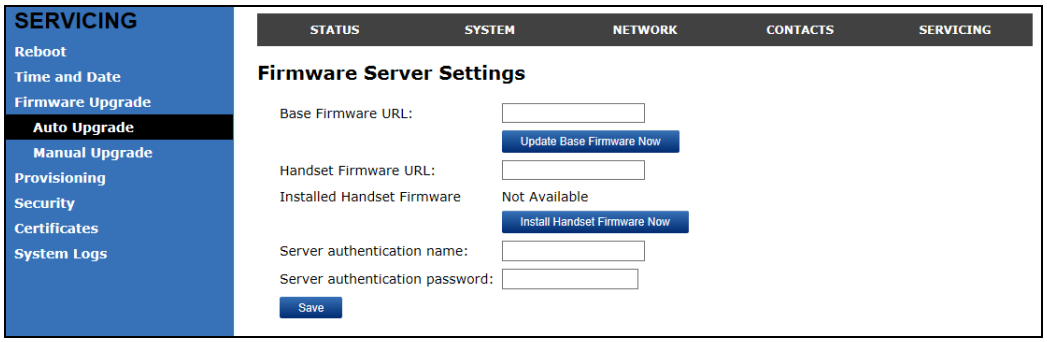
to start the VSP600 using the manual time settings.

Firmware Upgrade

You can update the VSP600 with new firmware using the following methods:

- Retrieving a firmware update file from a remote host computer and accessed via a URL. This central location may be arranged by you, an authorized dealer, or your SIP service provider. Enter the URL under **Firmware Server Settings**.
- Using a file located on your computer or local network. No connection to the Internet is required. Consult your dealer for access to firmware update files. Click **Manual Upgrade** to view the page where you can manually upgrade the VSP600 firmware.

The firmware upgrade settings are also available as parameters in the configuration file. See *“"provisioning" Module: Provisioning Settings” on page 98*.



Firmware Server Settings

Click the link for each setting to see the matching configuration file parameter in *“"provisioning" Module: Provisioning Settings” on page 98*. Default values and ranges are listed there.

Setting	Description
Base Firmware URL	The URL where the VSP600 Base Station firmware update file resides. This should be a full path, including the filename of the firmware file.
Handset Firmware URL	The URL where the VSP601 Cordless Handset firmware update file resides. This should be a full path, including the filename of the firmware file.
Server authentication name	Authentication username for the firmware server.
Server authentication password	Authentication password for the firmware server.

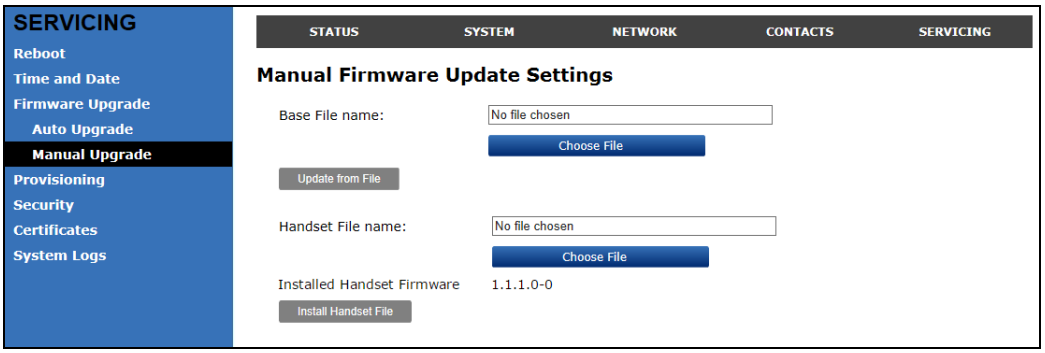
To update the firmware immediately:

- Click Update Base Firmware Now or Install Handset Firmware Now.

NOTE You can also configure the VSP600 to check for firmware updates at regular intervals. See *“Provisioning” on page 63*.

Manual Firmware Update and Upload

On the Manual Firmware Update Settings page, you can upgrade the VSP600 and handset firmware using a file located on your computer or local network.



To update the firmware using a file on your computer or local network:

1. On the Manual Firmware Update page, click Choose File to locate and open the firmware update file.
2. Click Update from File or Install Handset File.

After clicking Update from File the VSP600 will update its firmware and restart.

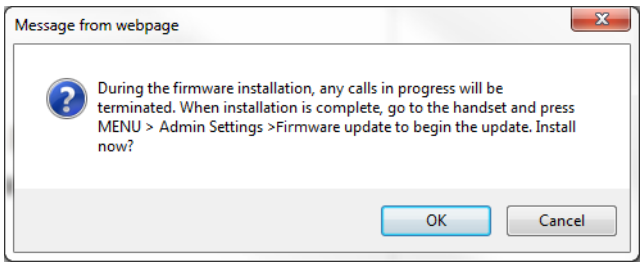
If you are updating handset firmware, you must perform one more step after clicking Install Handset File .

Updating a Cordless Handset

Updating DECT cordless handset firmware using the WebUI is a two-step process. First you must download the handset firmware and install it on the base station. Second, you must install the handset firmware on the handset. The handset downloads the firmware over the air from the base station.

To install the handset firmware on the basestation:

1. Click Install Handset Firmware Now for the Firmware Server update or Install Handset File for the Manual Firmware update.
   The confirmation dialog box shown below appears.



2. To install the handset firmware, click OK . The message **Installing handset firmware. Please wait...** appears. To cancel the download, click Cancel .

After clicking OK, the message **System update in progress. Please wait...** appears on the handset.

After a successful update, the message **Firmware installation successful** appears on the WebUI.

An error message appears if:

- the handset firmware is aleady up to date.
- the handset firmware URL is incorrect, or the file cannot be retrieved for any other reason.
- the handset firmware file is corrupted.
- the handset doesn‘t recognize the firmware file. For example, the firmware file may belong to a different ErisTerminal product.

To install the firmware on the cordless handset:

1. On the handset, press **MENU**, and then select **Admin settings**.
2. Enter the admin password. The default is **admin**. To switch between entering upper or lower-case letters, press the * key.
3. On the Admin settings menu, select **Firmware update**.
   The handset checks for new firmware. If new firmware is found, the handset screen asks you to proceed with the update.

NOTE Only one handset at a time can perform a firmware update. The base LEDs flash to indicate the base is busy and all incoming calls are rejected while the update is in progress.

Provisioning

Provisioning refers to the process of acquiring and applying new settings for the VSP600 using configuration files retrieved from a remote computer. After a VSP600 is deployed, subsequent provisioning can update the VSP600 with new settings; for example, if your service provider releases new features. See also *"Provisioning Using Configuration Files" on page 73*.

With automatic provisioning, you enable the VSP600 to get its settings automatically—the process occurs in the background as part of routine system operation. Automatic provisioning can apply to multiple devices simultaneously.

With manual provisioning on the WebUI, you update the VSP600 settings (configuration and/or firmware) yourself via **Provisioning > Import Configuration** and/or **Firmware Upgrade > Manual Upgrade**. Manual provisioning can only be performed on one VSP600 at a time.

On the Provisioning page, you can enter settings that will enable the VSP600 to receive automatic configuration and firmware updates. The Provisioning page also allows you to manually update VSP600 configuration from a locally stored configuration file using an Import function. You can also export the VSP600 configuration—either to back it up or apply the configuration to another VSP600 in the future—to a file on your computer.

The provisioning process functions according to the Resynchronization settings and Provisioning Server Settings. The VSP600 checks for the provisioning URL from the following sources in the order listed below:

1. PnP—Plug and Play Subscribe and Notify protocol

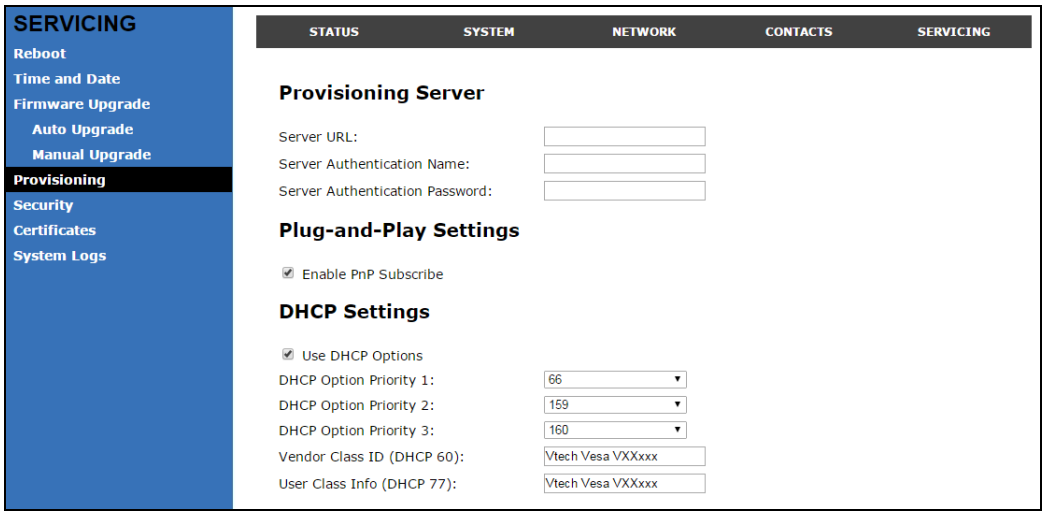
2. DHCP Options

3. Preconfigured URL—Any VSP600 updated to the latest firmware release will have the Redirection Server URL available as the default Provisioning Server URL (see *"provisioning.server_address" on page 98*).

Using the Redirection Service requires contacting the VTech support team for an account.

If one of these sources is disabled, not available, or has not been configured, the VSP600 proceeds to the next source until reaching the end of the list.

The provisioning settings are also available as parameters in the configuration file. See *""provisioning" Module: Provisioning Settings" on page 98*.



Provisioning Settings

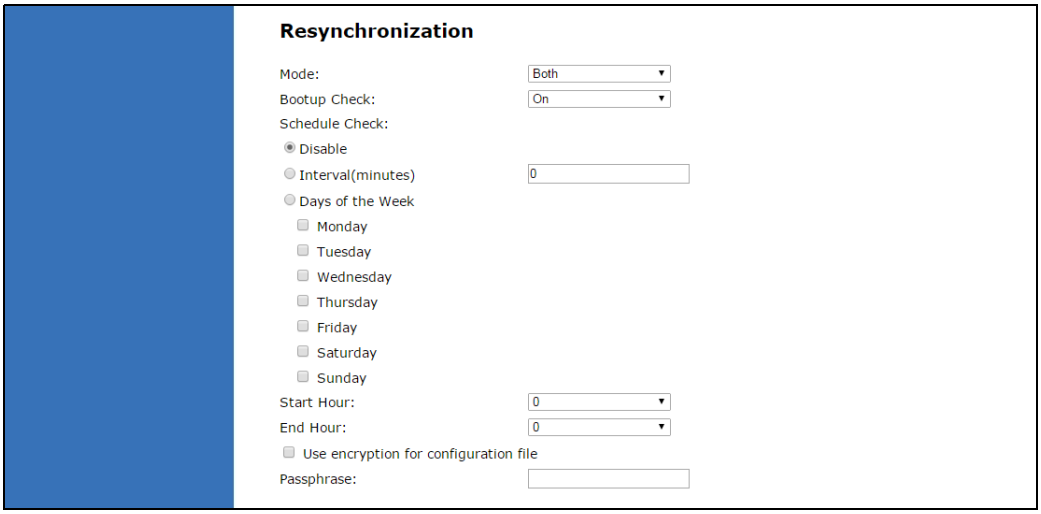
Setting	Description
Server URL	URL of the provisioning file(s). The format of the URL must be RFC 1738 compliant, as follows: "<schema>://<user>:<password>@ <host>:<port>/<url-path>" "<user>:<password>@" may be empty. "<port>" can be omitted if you do not need to specify the port number.
Server authentication name	User name for access to the provisioning server
Server authentication password	Password for access to the provisioning server

Plug-and-Play Settings

Setting	Description
Enable PnP Subscribe	Select to enable the VSP600 to search for the provisioning URL via a SUBSCRIBE message to a multicast address (224.0.1.75). The VSP600 expects the server to reply with a NOTIFY that includes the provisioning URL. The process times out after five attempts.

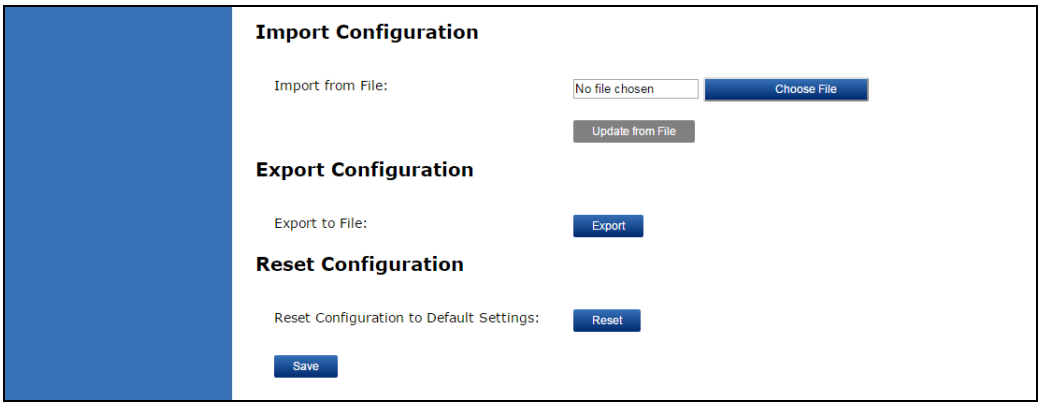
DHCP Settings

Setting	Description
Use DHCP Options	Enables the VSP600 to use DHCP options to locate and retrieve the configuration file. When selected, the VSP600 automatically attempts to get a provisioning server address, and then the configuration file. If DHCP options do not locate a configuration file, then the server provisioning string is checked. **Note**: Ensure that DHCP is also enabled on the “Basic Network Settings” page.
DHCP Option Priority 1	If DHCP is enabled, sets the DHCP Option priority. Select the highest priority option.
DHCP Option Priority 2	If DHCP is enabled, sets the DHCP Option priority. Select the second highest priority option.
DHCP Option Priority 3	If DHCP is enabled, sets the DHCP Option priority. Select the third highest priority option.
Vendor Class ID (DHCP 60)	DHCP Option 60 is available to send vendor-specific information to the DHCP Server.
User Class Info (DHCP 77)	DHCP Option 77 is available to send vendor-specific information to the DHCP Server.



Resynchronization

Setting	Description
Mode	Sets which files for which the VSP600 checks. It can check for configuration files, firmware update files (from the URL entered on the Firmware Server Settings page), or both. **Note**: When checking for both configuration and firmware files, the firmware URL can be within the config file. This firmware URL takes take precedence over the URL on the Firmware Server Settings page. It will also update the URL on the Firmware Server Settings page. This allows you to change the firmware URL automatically.
Bootup Check	Sets the VSP600 to check the provisioning URL for new configuration and/or firmware files upon bootup. The update is applied as part of the reboot process.
Schedule Check: Disable	When selected, disables regularly scheduled file checking.
Schedule Check: Interval	Sets an interval for checking for updates. After selecting Interval, enter the interval in minutes between update checks.
Schedule Check: Days of the Week	Select to enable weekly checking for updates on one or more days. After selecting Days of the Week, select the day(s) on which the VSP600 checks for updates.
Start Hour	Select the hour of the day on which the VSP600 checks for updates.
End Hour	Select the hour of the day on which the VSP600 stops checking for updates.
Use encryption	Enables an AES-encrypted configuration file to be decrypted before being applied to the VSP600. Select if the configuration file has been secured using AES encryption. See *"Securing configuration files with AES encryption" on page 79*.
Passphrase	If the configuration file has been secured using AES encryption, enter the 16-bit key. See *"Securing configuration files with AES encryption" on page 79*.



Import Configuration

You can configure the VSP600 by importing a configuration file from your computer or your local network. For more information about configuration file types and configuration file formatting, see *"Provisioning Using Configuration Files" on page 73*.

To import a configuration file:

1. Click Choose File to locate and open the configuration file.
2. Click Update from File .

The VSP600 will update its configuration.

Manually importing a configuration file differs from the auto-provisioning process in that:

- The VSP600 does not check whether the file has been loaded before. The configuration file is processed whether or not it is different from the current version.
- The VSP600 will restart immediately after importing the configuration file, without waiting for one minute of inactivity.

Export Configuration

You can export all the settings you have configured on the WebUI and save them as a configuration file on your computer. You can then use this configuration file as a backup, or use it to update other phones.

Under **Export Configuration**, you can also reset the phone to its default configuration.

NOTE

The exported configuration file will contain the following passwords in plain text:

- SIP account authentication password
- EAPOL password
- Firmware server password
- Provisioning server password
- Encryption passphrase
- LDAP server password

Please ensure that you save the exported configuration file in a secure location. You can also disable passwords from being exported as plain text. See *"provisioning.pwd_export_enable" on page 102*

To export the configuration file:

- Click Export .

The format of the exported file is **<model name>_<mac address>.cfg**. For example, **VSP600_0011A0OCF489.cfg**.

Exporting a configuration file generates two header lines in the configuration file. These header lines provide the model number and software version in the following format:

```
#Model Number = xxxxxxx

#SW Version = xxxxxxx
```

You can use the exported file as a general configuration file, and duplicate the settings across multiple units. However, ensure that you edit the file to remove any MAC-specific SIP account settings before applying the general configuration file to other units.

Reset Configuration

You can reset the phone to its default settings.

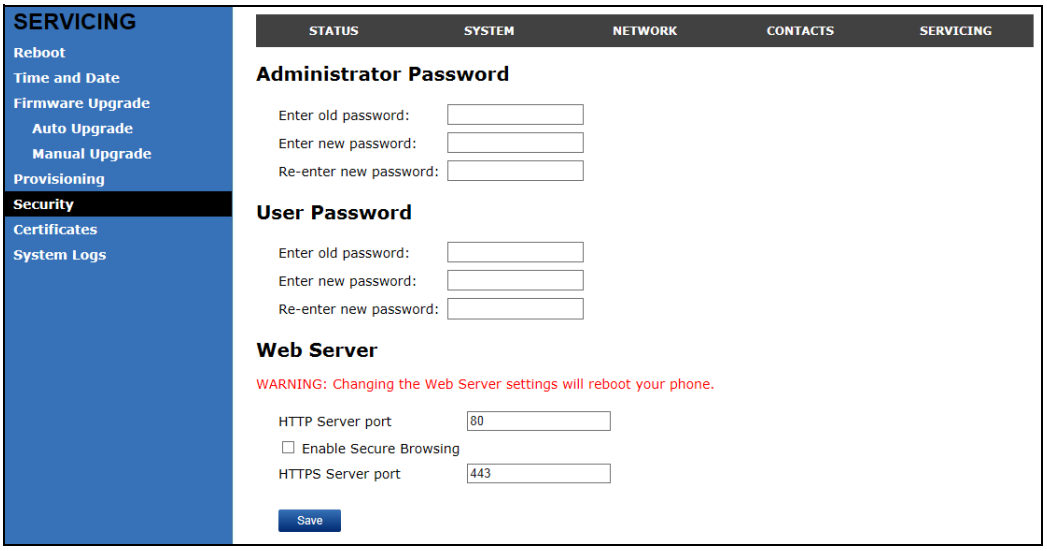
To reset the VSP600 to its default configuration:

1. Under **Reset Configuration**, click Reset .
2. When the confirmation box appears, click **OK**.

Security

On the **Security** page you can reset the admin password, reset the user password, and enter web server settings.

The security settings are also available as parameters in the configuration file. See *""web" Module: Web Settings" on page 112*.



Administrator Password

You can set the administrator password on the WebUI or by using provisioning. For more information on using provisioning to set the administrator password, see *""profile" Module: Password Settings" on page 121*.

To change the admin password:

1. Enter the old password (for a new VSP600, the default password is **admin**).
2. Enter and re-enter a new password. The password is case sensitive and can consist of both numbers and letters (to a maximum of 15 characters).
3. Click Save .

User Password

You can set the user password on the WebUI or by using provisioning. For more information on using provisioning to set the user password, see *""profile" Module: Password Settings" on page 121*.

To change the User password:

1. Enter the old password (for a new VSP600, the default password is **user**).
2. Enter and re-enter a new password. The password is case sensitive and can consist of both numbers and letters (to a maximum of 15 characters).
3. Click Save .

Web Server

Setting	Description
HTTP Server port	Port used by the HTTP server.
Enable Secure Browsing	Sets the server to use the HTTPS protocol.
HTTPS Server port	Port used by the HTTPS server.

To configure Web Server Settings:

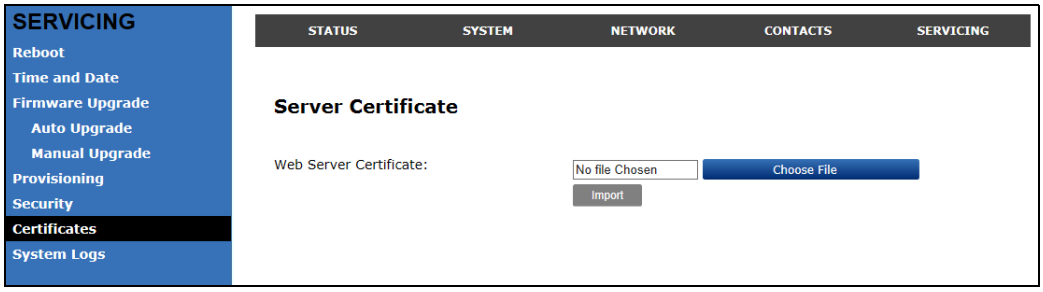
1. Enter the HTTP Server port number. The default setting is 80.
2. Enable or Disable Secure Browsing. When enabled, the HTTPS protocol is used, and you must select the HTTPS server port in the next step.
3. Enter the HTTPS server port number. The default setting is 443.

NOTE Changing the Web Server settings will reboot the VSP600.

Certificates

You can upload an optional web server certificate to the VSP600 to establish a secure connection between phone and server. If a certificate is not available, the VSP600's self-signed certificate will be used during the connection transaction.

A web server certificate can also be uploaded using provisioning. For more information, see *“"file" Module: Imported File Settings” on page 116*.



To upload a web server certificate:

1. On the Server Certificate page, click Choose File .
2. Locate the certificate file and click **Open**.
3. On the Server Certificate page, click Import .

System Logs

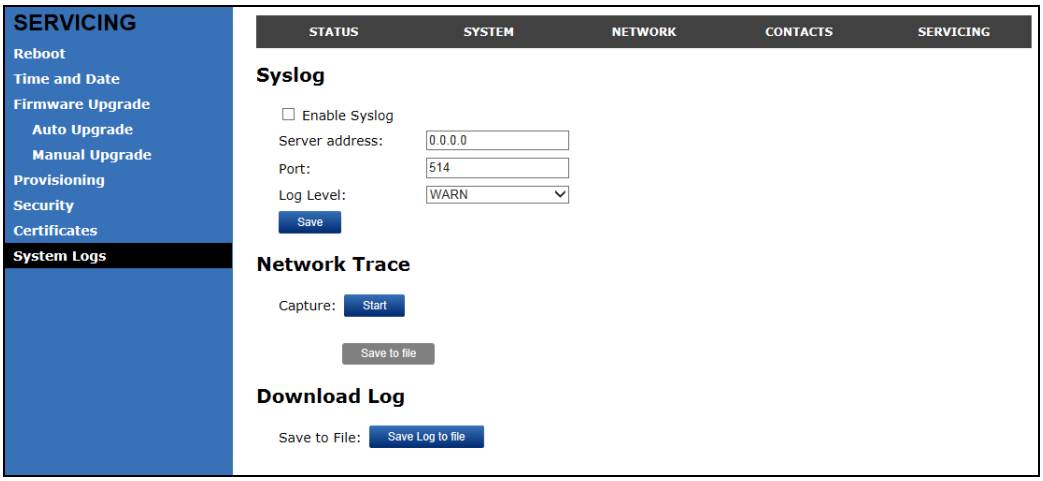
On the **Syslog Settings** page, you can enter settings related to system logging activities. It supports the following logging modes:

- Syslog server
- Volatile file

Under **Network Trace**, you can capture network traffic related to the phone's activity and save the capture as a .pcap file. The file can be used for diagnostic and troubleshooting purposes.

Under **Download Log**, you can save the system log to a file.

The Syslog settings are also available as parameters in the configuration file. See *“"log" Module: Log Settings” on page 107*.



Syslog Settings

Setting	Description
Enable Syslog	Enable log output to syslog server.
Server address	Syslog server IP address.
Server port	Syslog server port.
Log Level	Sets the log level. The higher the level, the larger the debug output. ■ 5—ALL ■ 4—DEBUG ■ 3—INFO ■ 2—WARNING ■ 1—ERROR ■ 0—CRITICAL

The logging levels are:

- CRITICAL: Operating conditions to be reported or corrected immediately (for example, an internal component failure or file system error).
- ERROR: Non-urgent failures—unexpected conditions that won't cause the device to malfunction.
- WARNING: An indication that an error or critical condition can occur if action is not taken.
- INFO: Normal operational messages.
- DEBUG: Developer messages for troubleshooting/debugging purposes.

Network Trace

To perform a network trace:

1. Start a network trace by clicking Start. The button changes to Stop.
2. Stop the network trace by clicking Stop.
3. Save the trace by clicking Save to file. Your browser should prompt you to save the **capture.pcap** file.

Download Log

To download the system log:

1. Click Save Log to file.
2. After your browser prompts you to save the **system.log** file, save the file in the desired location.

CHAPTER 4

PROVISIONING USING CONFIGURATION FILES

Provisioning using configuration files is the quickest way to configure multiple VSP600 base stations. You can place configuration files on a provisioning server, where the VSP600 base stations retrieve the files and update their configuration automatically.

Configuration files have the extension **.cfg** and contain settings that will apply to VSP600 base stations. To edit a configuration file, open it with a text editor such as Notepad.

The settings within a configuration file are grouped into modules. Most of the modules group their settings in the same way that settings are grouped on the VSP600 WebUI. For example, the "time_date" module in the configuration file contains the same settings that are on the **Time and Date** WebUI page. For a complete list of VSP600 configuration file modules and their associated parameters, see *"Configuration File Parameter Guide" on page 81*.

Using the WebUI, you can also import a configuration file and apply the configuration file settings to the VSP600. For more information, see *"Import Configuration" on page 67*.

This chapter covers:

The Provisioning Process

The automatic provisioning process is as follows:

1. Check for new or updated configuration files. For file-checking options, see *"Provisioning" on page 63* and *"Resynchronization: configuration file checking" on page 75*. The VSP600 maintains a list of the last loaded provisioning files. The VSP600 compares its current configuration against the files it finds on the provisioning server.

   If provisioning has been triggered by the resync timer expiring or by remote check-sync, the VSP600 checks for updated files after one minute of inactivity.

2. Download the configuration files.

   If any file on the provisioning server has changed, the VSP600 treats it as a new file and downloads it.

   If the provisioning URL specifies a path only with no filename, then by default the VSP600 looks for and retrieves the following two files:

   - General file: **<model>.cfg**.
   - MAC-specific file: **<model>_<MAC Address>.cfg**.

   The <model> variable is the VTech product model: VSP600, for example.

   If the provisioning URL specifies both a path and filename, then the VSP600 retrieves only the configuration file specified.

3. The VSP600 restarts after one minute of inactivity.

During provisioning, the VSP600 reads the configuration file and validates each module and setting. The VSP600 considers a setting valid if it is:

- a valid data type
- formatted as a valid setting
- within a valid data range
- part of a module that passes an integrity check. That is, the module's settings are consistent and logical. For example, in the "network" module, if DHCP is disabled, but no static IP address is specified, the module will fail the integrity check and none of the settings will apply.

Invalid modules or invalid settings are skipped and logged as ERROR messages in the system log, but will not interrupt the provisioning process. The system log will include the module parameters that have not been applied. A recognized module with unrecognized settings will cause all other settings in that module to be skipped.

A successful configuration or firmware update is reported as an INFO message in the system log.

See *"Configuration File Parameter Guide" on page 81* for the options and value ranges available for each configuration file setting.

Resynchronization: configuration file checking

You can select a number of options that determine when the VSP600 checks for new configuration files. This process of checking for configuration files is called Resynchronization. Resynchronization options are available on the WebUI **Provisioning** page, but you can also include them in a configuration file.

The resynchronization options are:

- Mode—sets the VSP600 to check for a configuration file only, a firmware update file only, or both types of file.
- Never—configuration file checking is disabled
- Bootup—the VSP600 checks for new configuration files when it boots up. Any updates are applied during the boot-up process.
- Remote check-sync—enables you to start a resynchronization remotely using your hosted server's web portal. The Remote check-sync settings are available only in the configuration file, not the WebUI.
- Repeatedly, at a defined interval from 60 to 65535 minutes (45 days).

VSP600 restart

If the VSP600 needs to restart after an auto-update, the restart happens only after the device has been idle for one minute.

To prevent users from delaying the update process (auto-updates cannot begin until the VSP600 has been idle for one minute), or to avoid device restarts that might interfere with incoming calls:

- set the resynchronization interval to a suitable period
- upload any new configuration file(s) to your provisioning server after work hours so that the VSP600 will download the file(s) when there is no call activity.

When you update the VSP600 by importing a configuration file using the WebUI, the device restarts immediately after applying the new settings, regardless of whether the VSP600 is idle.

Configuration File Types

The VSP600 is able to retrieve and download two types of configuration file. Depending on your requirements, you may want to make both types of configuration file available on your provisioning server.

The two configuration file types are a general configuration file and a MAC-specific configuration file. The types differ in name only. The formatting of the files' content is the same.

The general configuration file contains settings that are required by every VSP600 in the system.

The MAC-specific configuration file is a file that only a single VSP600 can retrieve. The MAC-specific configuration file name contains a VSP600 MAC address and can only be retrieved by the device with a matching MAC address.

The filename formats for both files are:

- General file: **<model>.cfg**
- MAC-specific file: **<model>_<MAC Address>.cfg**

The <model> variable is the VTech product model; for example, **VSP600**. For more information about the MAC-specific configuration file, see *"Guidelines for the MAC-Specific configuration file" on page 78*.

If the provisioning URL specifies a path only with no filename, then by default the VSP600 will fetch both files.

However, if the provisioning URL specifies both a path and filename, then the VSP600 will only fetch the single configuration file specified.

Both the general and MAC-specific files can contain any of the available configuration settings. A setting can appear in the general configuration file or the MAC-specific configuration file, or both files, or neither file. If a setting appears in both files, the setting that is read last is the one that applies.

When the VSP600 fetches both a general and a MAC-specific configuration file, the general file is processed first. You can configure a setting for most of your VSP600 base stations in the general file, and then overwrite that setting for just a few VSP600 base stations using the MAC-specific file.

Data Files

The configuration file can also include links to data files for product customization. Allowed data types include the following:

- Directory (contacts, blacklist) in .xml format
- Certificates (server, provisioning) in pem format

Links to data files are in the configuration file's "file" module. This is where you enter any URLs to the data files that the VSP600 base station may require.

None of the data files are exported when you export a configuration file from the VSP600. However, you can export a Directory or Blacklist .xml file using the WebUI. After modifying the .xml file, you can use the configuration file "file" module to have the VSP600 import the new file. For a complete list of data file parameters, see *""file" Module: Imported File Settings" on page 116*.

Configuration File Tips and Security

All configuration settings are initially stored in a configuration template file. Copy, rename, and edit the template file to create a general configuration file and the MAC-specific configuration files you will need. You can store the general configuration file and the MAC-specific files on your provisioning server.

Do not modify the configuration file header line that includes the model and firmware version.

To save yourself time and effort, consider which settings will be common to all (or the majority of) VSP600 base stations. Such settings might include call settings, language, and NAT settings. You can then edit those settings in the configuration template and save it as the general configuration file. The remaining settings will make up the MAC-specific configuration file, which you will have to copy and edit for each VSP600.

Guidelines for the MAC-Specific configuration file

The VSP600 downloads the MAC-specific configuration file after the general configuration file. You must create a MAC-specific configuration file for each VSP600 in your system. The file name must contain the VSP600 MAC address, which is printed on a label on the bottom of the device. For example, a VTech VSP600 base station with the MAC address of 00:11:A0:10:6F:2D would download the **VSP600_0011A0106F2D.cfg** file.

When renaming a MAC-specific configuration file, ensure the filename is all upper case.

The MAC-specific configuration file contains settings intended exclusively for that VSP600 base station. Such settings will include SIP account settings such as display name, user ID, and authentication ID.

Securing configuration files with AES encryption

You can encrypt your configuration files to prevent unauthorized users modifying the configuration files. The VSP600 firmware decrypts files using the AES 256 algorithm. After encrypting a file and placing it on your provisioning server, you can enable the VSP600 to decrypt the file after fetching it from the server.

The procedures in this section use OpenSSL for Windows for file encryption, as shown in Figure 2.

To decrypt a configuration file, you will need a 16-character AES key that you specified when you encrypted the file. The key (or passphrase) is limited to 16 characters in length and supports special characters **~ ^ ` % ! & - _ + = | . @ * : ; , ? ( ) [ ] { } < > / \ #** as well as spaces.

NOTE The encryption of configuration files is supported only for the auto provisioning process. Encrypt files only if you intend to store them on a provisioning server. Do not encrypt files that you intend to manually import to the VSP600. You cannot enable decryption for manually imported configuration files.

To encrypt a configuration file:

1. (Optional) Place your configuration file in the same folder as the openssl executable file. If the configuration file is not in the same folder as the openssl executable file, you can enter a relative pathname for the [infile] in the next step.
2. Double-click the **openssl.exe** file.
3. On the openssl command line, type:

   ```
   enc -aes-256-cbc -pass pass:[passphrase123456] -in [infile] -out [outfile]
   -nosalt -p
   ```

Elements in brackets are examples—do not enter the brackets. Enter a 16-character passphrase and the unencrypted configuration file filename (the "infile") and a name for the encrypted file ("outfile") that will result.

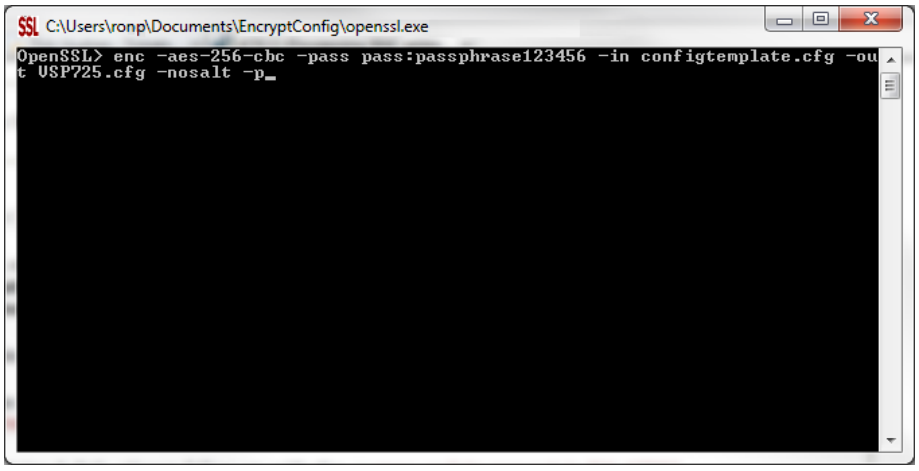
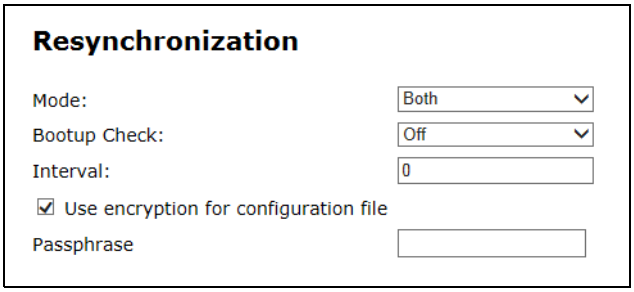


Figure 2. OpenSSL command line

To enable configuration file decryption:

1. On the WebUI, click **Servicing > Provisioning**.
2. On the Provisioning page under **Resynchronization**, select **Use Encryption for configuration file**.



3. Enter the 16-character passphrase that you created when you encrypted the configuration file.
4. Click Save .

NOTE You must ensure that configuration files are encrypted when enabling AES Encryption. Decrypting an unencrypted file will result in a garbage file that is not processed. This will also be logged as an error in the system log.

CHAPTER 5

CONFIGURATION FILE PARAMETER GUIDE

This chapter lists the available options for all the settings within the VSP600 configuration file. Most settings in the configuration file have an equivalent in the WebUI (see the settings tables in *“Using the WebUI” on page 25*). However, the options you must enter when editing the configuration file have a different syntax and format.

The settings are divided into modules. Most modules correspond to a page on the VSP600 WebUI. You may wish to reorganize the modules within the configuration file itself. The configuration file settings can be listed in any order, and the configuration file will still be valid.

The modules included in the configuration file are:

"sip_account" Module: SIP Account Settings

The SIP Account settings enable you to set up individual accounts for each user. You can add up to three accounts for each VSP600. Each account requires you to configure the same group of SIP account settings. The SIP account settings for each account are identified by the account number, from 1 to 6 for the VSP600.

For example, for account 1 you would set:

```
sip_account.1.sip_account_enable = 1

sip_account.1.label = Line 1

sip_account.1.display_name = 1001

sip_account.1.user_id = 2325551001
```

and so on.

For account 2, you would set:

```
sip_account.2.sip_account_enable = 1

sip_account.2.label = Line 2

sip_account.2.display_name = 1002

sip_account.2.user_id = 2325551002
```

and so on, if you have additional accounts to configure.

The SIP account settings follow the format: sip_account.x.[element], where x is an account number ranging from 1 to 6 for the VSP600.

All these settings are exported when you manually export the configuration from the VSP600.

General configuration file settings

Setting:	**sip_account.x.dial_plan**		
Description:	Sets the dial plan for account x. See *"Dial Plan" on page 32*.		
Values:	Text string	**Default:**	x+P

Setting:	**sip_account.x.inter_digit_timeout**		
Description:	Sets the inter-digit timeout (in seconds) for account x. The inter-digit timeout sets how long the VSP600 waits after the last digit is entered before dialing the number.		
Values:	1–10	**Default:**	3

Setting:	**sip_account.x.maximum_call_number**		
Description:	Sets the maximum number of concurrent active calls allowed for that account.		
Values:	1–4	**Default:**	4

Setting:	**sip_account.x.dtmf_transport_method**		
Description:	Sets the transport method for DTMF signalling for account x.		
Values:	auto, rfc2833, inband, info	**Default:**	auto

Setting:	**sip_account.x.unregister_after_reboot_enable**		
Description:	Enables or disables the VSP600 to unregister account x after rebooting.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.primary_sip_server_address**		
Description:	Sets the SIP server IP address for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.primary_sip_server_port**		
Description:	Sets the SIP server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	**sip_account.x.primary_registration_server_address**		
Description:	Sets the registration server IP address for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.primary_registration_server_port**		
Description:	Sets the registration server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	**sip_account.x.primary_registration_expires**		
Description:	Sets the expiration time (in seconds) of the current registration for account x.		
Values:	30–7200	**Default:**	3600

Setting:	**sip_account.x.registration_retry_time**		
Description:	Sets the retry frequency of the current registration for account x.		
Values:	1–1800	**Default:**	10

Setting:	**sip_account.x.primary_outbound_proxy_server_address**		
Description:	Sets the outbound proxy server IP address for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.primary_outbound_proxy_server_port**		
Description:	Sets the outbound proxy server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	**sip_account.x.backup_outbound_proxy_server_address**		
Description:	Sets the backup outbound proxy server IP address for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.backup_outbound_proxy_server_port**		
Description:	Sets the backup outbound proxy server port for account x.		
Values:	1–65535	**Default:**	5060

Setting:	**sip_account.x.codec_priority.1**		
Description:	Sets the highest-priority codec for account x.		
Values:	g711u, g711a, g729, g726, g722	**Default:**	g711u

Setting: `sip_account.x.codec_priority.2`

Description: Sets the second highest-priority codec for account x.

Values: none, g711u, g711a, g729, g726, g722 **Default:** g711a

Setting: `sip_account.x.codec_priority.3`

Description: Sets the third highest-priority codec for account x.

Values: none, g711u, g711a, g729, g726, g722 **Default:** g726

Setting: `sip_account.x.codec_priority.4`

Description: Sets the fourth highest-priority codec for account x.

Values: none, g711u, g711a, g729, g726, g722 **Default:** g722

Setting: `sip_account.x.codec_priority.5`

Description: Sets the fifth highest-priority codec for account x.

Values: none, g711u, g711a, g729, g726, g722 **Default:** g729

Setting: `sip_account.x.voice_encryption_enable`

Description: Enables or disables SRTP voice encryption for account x.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.g729_annexb_enable`

Description: Enables G.729 Annex B, with voice activity detection (VAD) and bandwidth-conserving silence suppression. This setting applies only when G.729a/b is selected in a `sip_account.x.codec_priority` parameter.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.dscp`

Description: Sets the Voice Quality of Service Layer 3 - DSCP for account x.

Values: 0–63 **Default:** 46

Setting:	**sip_account.x.sip_dscp**		
Description:	Sets the Signalling Quality of Service Layer 3 - DSCP for account x.		
Values:	0–63	**Default:**	26

Setting:	**sip_account.x.normal_jitter**		
Description:	Sets the oRTP jitter buffer in milliseconds.		
Values:	30–500	**Default:**	80

Setting:	**sip_account.x.local_sip_port**		
Description:	Sets the Local SIP port for account x.		
Values:	1–65535	**Default:**	Account 1: 5060 Account 2: 5070 Account 3: 5080 Account 4: 5090 Account 5: 5100 Account 6: 5200

Setting:	**sip_account.x.transport_mode**		
Description:	Sets the Signalling Transport Mode for account x.		
Values:	udp, tcp, tls	**Default:**	udp

Setting:	**sip_account.x.access_code_retrieve_voicemail**		
Description:	Sets the voicemail retrieval feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_dnd_on**		
Description:	Sets the do not disturb (DND) ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_dnd_off**		
Description:	Sets the do not disturb (DND) OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_cfa_on**		
Description:	Sets the Call Forward All ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_cfa_off**		
Description:	Sets the Call Forward All OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_cfna_on**		
Description:	Sets the Call Forward No Answer ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_cfna_off**		
Description:	Sets the Call Forward No Answer OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_cfb_on**		
Description:	Sets the Call Forward Busy ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_cfb_off**		
Description:	Sets the Call Forward Busy OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_anonymous_call_block_on**		
Description:	Sets the Anonymous Call Block ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_anonymous_call_block_off**		
Description:	Sets the Anonymous Call Block OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_outgoing_call_anonymous_on**		
Description:	Sets the Anonymous Outgoing Call ON feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.access_code_outgoing_call_anonymous_off**		
Description:	Sets the Anonymous Outgoing Call OFF feature access code for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.mwi_enable**		
Description:	Enables or disables message waiting indicator subscription for account x. Enable if SUBSCRIBE and NOTIFY methods are used for MWI.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.mwi_subscription_expires**		
Description:	Sets the MWI subscription expiry time (in seconds) for account x.		
Values:	0–65535	**Default:**	3600

Setting:	**sip_account.x.mwi_ignore_unsolicited**		
Description:	Enables or disables ignoring of unsolicited MWI notifications—notifications in addition to, or instead of, SUBSCRIBE and NOTIFY methods—for account x. Disable if MWI service is configured on the voicemail server and does not involve a subscription to a voicemail server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.nat_traversal_stun_enable**		
Description:	Enables or disables STUN (Simple Traversal of UDP through NATs) for account x. STUN enables clients, each behind a firewall, to establish calls via a service provider hosted outside of either local network.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.nat_traversal_stun_server_address**		
Description:	Sets the STUN server IP address.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.nat_traversal_stun_server_port**		
Description:	Sets the STUN server port.		
Values:	1–65535	**Default:**	3478

Setting:	**sip_account.x.nat_traversal_udp_keep_alive_enable**		
Description:	Enables or disables UDP keep-alives. Keep-alive packets are used to maintain connections established through NAT.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**sip_account.x.nat_traversal_udp_keep_alive_interval**		
Description:	Sets the interval (in seconds) for sending UDP keep-alives.		
Values:	0–65535	**Default:**	30

Setting:	**sip_account.x.music_on_hold_enable**		
Description:	Enables or disables a hold-reminder tone that a far-end caller hears when put on hold during a call on account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**sip_account.x.network_conference_enable**		
Description:	Enables or disables network conferencing for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.network_bridge_uri**		
Description:	Sets the URI for the network conferencing bridge on account x.		
Values:	Text string (SIP URI)	**Default:**	Blank

Setting:	**sip_account.x.sip_session_timer_enable**		
Description:	Enables or disables the SIP session timer.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.sip_session_timer_min**		
Description:	Sets the session timer minimum value (in seconds) for account x.		
Values:	90–65535	**Default:**	90

Setting:	**sip_account.x.sip_session_timer_max**		
Description:	Sets the session timer maximum value (in seconds) for account x.		
Values:	0–65535	**Default:**	1800

Setting:	**sip_account.x.check_trusted_certificate**		
Description:	Enables or disables accepting only a trusted TLS certificate for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.use_first_trusted_certificate_for_all**		
Description:	Enables or disables accepting the first TLS certificate for all accounts.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.preferred_ptime**		
Description:	Enter the packetization interval time in milliseconds.		
Values:	10, 20, 30, 40, 50, 60	**Default:**	20

Setting:	**sip_account.x.call_rejection_response_code**		
Description:	Select the response code for call rejection. This code applies to the following call rejection cases: ■ User presses **Reject** for an incoming call ■ DND is enabled ■ Phone rejects a second incoming call with Call Waiting disabled ■ Phone rejects an anonymous call with Anonymous Call Rejection enabled ■ Phone rejects call when the maximum number of calls is reached		
Values:	480, 486, 603	**Default:**	486

MAC-specific configuration file settings

Setting: `sip_account.x.sip_account_enable`

Description: Enables account x to be used by the device.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: `sip_account.x.label`

Description: Sets the text that identifies the account on the device LCD. The account label appears on the Dialing Line list, dialing screen, and other call appearance screens.

Values: Text string **Default:** Blank

Setting: `sip_account.x.display_name`

Description: Sets the text portion of the caller ID that is displayed for outgoing calls using account x.

Values: Text string **Default:** Blank

Setting: `sip_account.x.user_id`

Description: Sets the account ID for account x. Depending on your service provider's specifications, this could be an extension number.
Note: Do not enter the host name (e.g. "@sipservice.com"). The configuration file automatically adds the default host name.

Values: Text string **Default:** Blank

Setting: `sip_account.x.authentication_name`

Description: Sets the authentication name for account x. Depending on your service provider's specifications, this could be identical to the user ID.

Values: Text string **Default:** Blank

Setting: `sip_account.x.authentication_access_password`

Description: Sets the authentication password for account x.

Values: Text string **Default:** Blank

Setting:	**sip_account.x.feature_sync_enable**		
Description:	Enables or disables feature synchronization for account x. When enabled, features configured on the service provider's web portal will automatically be updated on the device's WebUI.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.mwi_uri**		
Description:	Sets the MWI URI that will be used for MWI subscription. If this setting is left blank, the VSP600 uses the account x user ID for MWI subscription.		
Values:	SIP URI text string	**Default:**	Blank

"hs_settings" Module: Handset Settings

The Handset Settings allow you to configure account assignments and names for the cordless handsets that are registered to the base station. For more information on registering cordless handsets, see the VSP600/VSP601 User Guide.

General configuration file settings

Setting: `hs_settings.x.handset_us_pin_code`

Description: Sets the new 4-digit PIN for handset registration/deregistration.

Values: 4-digit number **Default:** 1592

MAC-specific configuration file settings

Setting: `hs_settings.x.handset_name`

Description: Sets the name for handset x. You can use up to 11 letters and/or numbers. Use alphanumeric characters only—no symbol characters are allowed.

Values: Text string **Default:** HANDSET

Setting: `hs_settings.x.default_account`

Description: Sets the default account for handset x. The handset attempts to use this account first when going off hook.

Values: 1–6 **Default:** 1

Setting: `hs_settings.x.assigned_account`

Description: Sets the accounts for handset x that will be available for incoming and outgoing calls. List account numbers separated by commas (for example, 1,2,3,4,5,6).

Values: 1–6 **Default:** 1,2,3,4,5,6

"network" Module: Network Settings

The network settings follow the format: network.[element].

General configuration file settings

Setting:	**network.rtp.port_start**		
Description:	Sets the Local RTP port range start.		
Values:	1–65535	**Default:**	18000

Setting:	**network.rtp.port_end**		
Description:	Sets the Local RTP port range end.		
Values:	1–65535	**Default:**	19000

Setting:	**network.vlan.wan.enable**		
Description:	Enables or disables the WAN VLAN.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**network.vlan.wan.id**		
Description:	Sets the WAN VLAN ID.		
Values:	0–4095	**Default:**	0

Setting:	**network.vlan.wan.priority**		
Description:	Sets the WAN port priority.		
Values:	0–7	**Default:**	0

Setting:	**network.lldp_med.enable**		
Description:	Enables or disables LLDP-MED.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**network.lldp_med.interval**		
Description:	Sets the LLDP-MED packet interval (in seconds).		
Values:	1–30	**Default:**	10

Setting:	**network.eapol.enable**		
Description:	Enables or disables 802.1x EAPOL.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**network.eapol.identity**		
Description:	Sets the 802.1x EAPOL identity.		
Values:	Text string	**Default:**	Blank

Setting:	**network.eapol.access_password**		
Description:	Sets the 802.1x EAPOL MD5 password.		
Values:	Text string	**Default:**	Blank

Setting:	**network.vendor_class_id**		
Description:	Sets the vendor ID for DHCP option 60.		
Values:	Text string	**Default:**	Vtech Vesa VSP600

Setting:	**network.user_class**		
Description:	Sets the user class for DHCP option 77.		
Values:	Text string	**Default:**	Vtech Vesa VSP600

Setting:	**network.ip_dns_cache_clear_timeout**		
Description:	Sets the interval (in minutes) between removing all caching and performing a new DNS lookup. Set to 0 to remove all caching and perform a DNS lookup for every outgoing request and response (TTL=0 emulation).		
Values:	0–1440	**Default:**	60

MAC-specific configuration file settings

Setting:	**network.nat.masquerading_enable**		
Description:	Enables or disables IP masquerading.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**network.nat.public_ip_addr**		
Description:	Sets the public IP address.		
Values:	Text string (IPv4)	**Default:**	0

Setting:	**network.nat.public_sip_port**		
Description:	Sets the public SIP port.		
Values:	1–65535	**Default:**	5060

Setting:	**network.nat.public_rtp_port_start**		
Description:	Sets the public RTP port range start.		
Values:	1–65535	**Default:**	18000

Setting:	**network.nat.public_rtp_port_end**		
Description:	Sets the public RTP port range end.		
Values:	1–65535	**Default:**	19000

Setting:	**network.ip.dhcp_enable**		
Description:	Indicates whether DHCP is enabled.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**network.ip.static_ip_addr**		
Description:	Sets a static IP address for the network.		
Values:	Text string (IPv4)	**Default:**	Blank

Setting:	**network.ip.subnet_mask**		
Description:	Sets the subnet mask for the network.		
Values:	Text string (IPv4)	**Default:**	Blank

Setting:	**network.ip.gateway_addr**		
Description:	Sets the Gateway IP address.		
Values:	Text string (IPv4)	**Default:**	Blank

Setting:	**network.ip.dns1**		
Description:	Sets the primary DNS server IP address.		
Values:	Text string (IPv4)	**Default:**	Blank

Setting:	**network.ip.dns2**		
Description:	Sets the secondary DNS server IP address.		
Values:	Text string (IPv4)	**Default:**	Blank

"provisioning" Module: Provisioning Settings

The provisioning settings follow the format: provisioning.[element].

All these settings are exported when you manually export the configuration from the VSP600.

All the provisioning settings are included in the general configuration file.

Setting:	**`provisioning.firmware_url`**		
Description:	Sets the URL for the server hosting the firmware file.		
Values:	Text string	**Default:**	Blank

Setting:	**`provisioning.handset_firmware_url`**		
Description:	Sets the URL for the server hosting the handset firmware file.		
Values:	Text string	**Default:**	Blank

Setting:	**`provisioning.fw_server_username`**		
Description:	Sets the authentication name for the server hosting the firmware file.		
Values:	Text string	**Default:**	Blank

Setting:	**`provisioning.fw_server_access_password`**		
Description:	Sets the authentication password for the server hosting the firmware file.		
Values:	Text string	**Default:**	Blank

Setting:	**`provisioning.server_address`**		
Description:	Sets the provisioning server IP address.		
Values:	Text string	**Default:**	http://et.vtechphones.com/redirectserver

Setting:	**`provisioning.server_username`**		
Description:	Sets the authentication name for the provisioning server.		
Values:	Text string	**Default:**	Blank

Setting:	**provisioning.server_access_password**		
Description:	Sets the authentication password for the provisioning server.		
Values:	Text string	**Default:**	Blank

Setting:	**provisioning.dhcp_option_enable**		
Description:	Enables or disables using DHCP options for locating the configuration and firmware files.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**provisioning.dhcp_option_priority_1**		
Description:	Sets the first priority DHCP option for the provisioning/firmware file check.		
Values:	66, 159, 160	**Default:**	66

Setting:	**provisioning.dhcp_option_priority_2**		
Description:	Sets the second priority DHCP option for the provisioning/firmware file check.		
Values:	66, 159, 160	**Default:**	159

Setting:	**provisioning.dhcp_option_priority_3**		
Description:	Sets the third priority DHCP option for the provisioning/firmware file check.		
Values:	66, 159, 160	**Default:**	160

Setting:	**provisioning.resync_mode**		
Description:	Sets the mode of the device's provisioning/firmware file check. This determines which files the device retrieves when the resync process begins.		
Values:	config_only, firmware_only, config_and_firmware	**Default:**	config_and_firmware

Setting:	**provisioning.bootup_check_enable**		
Description:	Enables or disables bootup check for configuration and firmware files.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**provisioning.schedule_mode**		
Description:	Sets the type of schedule check for configuration and firmware files.		
Values:	disable, interval, weekday	**Default:**	disable

Setting:	**provisioning.resync_time**		
Description:	Sets the interval (in minutes) between checks for new firmware and/or configuration files.		
Values:	0–65535	**Default:**	0 (OFF)

Setting:	**provisioning.weekdays**		
Description:	Sets the day(s) when the device checks for new firmware and/or configuration files. Enter a comma-delimited list of weekdays from 0 (Sunday) to 6 (Saturday). For example, 5,6,0 means the provisioning check will be performed on Friday, Saturday and Sunday.		
Values:	0–6	**Default:**	Blank

Setting:	**provisioning.weekdays_start_hr**		
Description:	Sets the hour when the device checks for new firmware and/or configuration files.		
Values:	0–23	**Default:**	0

Setting:	**provisioning.weekdays_end_hr**		
Description:	Sets the hour when the device stops checking for new firmware and/or configuration files.		
Values:	0–23	**Default:**	0

Setting:	**provisioning.remote_check_sync_enable**		
Description:	Enables or disables remotely triggering the device to check for new firmware and/or configuration files. The file checking is triggered remotely via a SIP Notify message from the server containing the **check-sync** event.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**provisioning.crypto_enable**
Description:	Enables or disables encryption check for the configuration file(s). Enable if you have encrypted the configuration file(s) using AES encryption.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	**provisioning.crypto_passphrase**
Description:	Sets the AES encryption passphrase for decrypting the configuration file(s). Enter the key that was generated when you encrypted the file.
Values:	Text string **Default:** Blank

Setting:	**provisioning.check_trusted_certificate**
Description:	Enables or disables accepting only a trusted TLS certificate for access to the provisioning server.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	**provisioning.pnp_enable**
Description:	Enables or disables the VSP600 checking for the provisioning URL using the Plug-and-Play Subscribe and Notify protocol.
Values:	0 (disabled), 1 (enabled) **Default:** 1

Setting:	**provisioning.pnp_response_timeout**
Description:	Sets how long the VSP600 repeats the SUBSCRIBE request if there is no reply from the PnP server.
Values:	1–60 **Default:** 10

Setting:	**`provisioning.pwd_export_enable`**
Description:	Enables or disables passwords from being exported in plain text. This parameter is not available on the WebUI. The passwords affected are: ■ network.eapol.access_password ■ provisioning.fw_server_access_password ■ provisioning.server_access_password ■ profile.admin.access_password ■ profile.user.access_password ■ sip_account.x.authentication_access_password ■ remoteDir.ldap_access_password ■ remoteDir.broadsoft_access_password
Values:	0 (disabled), 1 (enabled) **Default:** 0

"time_date" Module: Time and Date Settings

The time and date settings follow the format: time_date.[element].

All these settings are exported when you manually export the configuration from the VSP600.

All the time and date settings are included in the general configuration file.

Setting:	`time_date.ntp_server`		
Description:	Enables or disables NTP server to set time and date.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	`time_date.ntp_server_addr`		
Description:	Sets the URL for the NTP server.		
Values:	Text string	**Default:**	us.pool.ntp.org

Setting:	`time_date.ntp_dhcp_option`		
Description:	Enables or disables DHCP option 42 to find the NTP server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`time_date.selected_timezone`
Description:	Sets the local timezone.

Values: Pacific/Pago_Pago, Pacific/Honolulu, America/Adak, America/Anchorage, America/Vancouver, America/Tijuana, America/Los_Angeles, America/Edmonton, America/Chihuahua, America/Denver, America/Phoenix, America/Winnipeg, Pacific/Easter, America/Mexico_City, America/Chicago, America/Nassau, America/Montreal, America/Grand_Turk, America/Havana, America/New_York, America/Caracas, America/Halifax, America/Santiago, America/Asuncion, Atlantic/Bermuda, Atlantic/Stanley, America/Port_of_Spain, America/St_Johns, America/Godthab, America/Argentina/Buenos_Aires, America/Fortaleza, America/Sao_Paulo, America/Noronha, Atlantic/Azores, GMT, America/Danmarkshavn, Atlantic/Faroe, Europe/Dublin, Europe/Lisbon, Atlantic/Canary, Europe/London, Africa/Casablanca, Europe/Tirane, Europe/Vienna, Europe/Brussels, Europe/Zagreb, Europe/Prague, Europe/Copenhagen, Europe/Paris, Europe/Berlin, Europe/Budapest, Europe/Rome, Europe/Luxembourg, Europe/Skopje, Europe/Amsterdam, Africa/Windhoek, Europe/Tallinn, Europe/Helsinki, Asia/Gaza, Europe/Athens, Asia/Jerusalem, Asia/Amman, Europe/Riga, Asia/Beirut, Europe/Chisinau, Europe/Kaliningrad, Europe/Bucharest, Asia/Damascus, Europe/Istanbul, Europe/Kiev, Africa/Djibouti, Asia/Baghdad, Europe/Moscow, Asia/Tehran, Asia/Yerevan, Asia/Baku, Asia/Tbilisi, Asia/Aqtau, Europe/Samara, Asia/Aqtobe, Asia/Bishkek, Asia/Karachi, Asia/Yekaterinburg, Asia/Kolkata, Asia/Almaty, Asia/Novosibirsk, Asia/Krasnoyarsk, Asia/Bangkok, Asia/Shanghai, Asia/Singapore, Australia/Perth, Asia/Seoul, Asia/Tokyo, Australia/Adelaide, Australia/Darwin, Australia/Sydney, Australia/Brisbane, Australia/Hobart, Asia/Vladivostok, Australia/Lord_Howe, Pacific/Noumea, Pacific/Auckland, Pacific/Chatham, Pacific/Tongatapu

Default: America/New_York

Setting:	**time_date.daylight_saving_auto_adjust**		
Description:	Sets the device to automatically adjust clock for daylight savings.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**time_date.daylight_saving_user_defined**		
Description:	Enables or disables manual daylight savings configuration.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**time_date.daylight_saving_start_month**		
Description:	Sets the month that daylight savings time starts.		
Values:	January–December	**Default:**	March

Setting:	**time_date.daylight_saving_start_week**		
Description:	Sets the week that daylight savings time starts.		
Values:	1–5	**Default:**	2

Setting:	**time_date.daylight_saving_start_day**		
Description:	Sets the day that daylight savings time starts.		
Values:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	**Default:**	Sunday

Setting:	**time_date.daylight_saving_start_hour**		
Description:	Sets the hour that daylight savings time starts.		
Values:	00:00–23:00	**Default:**	02:00

Setting:	**time_date.daylight_saving_end_month**		
Description:	Sets the month that daylight savings time ends.		
Values:	January–December	**Default:**	November

Setting:	**time_date.daylight_saving_end_week**		
Description:	Sets the week that daylight savings time ends.		
Values:	1–5	**Default:**	1

Setting:	**time_date.daylight_saving_end_day**		
Description:	Sets the day that daylight savings time ends.		
Values:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	**Default:**	Sunday

Setting:	**time_date.daylight_saving_end_hour**		
Description:	Sets the hour that daylight savings time ends.		
Values:	00:00–23:00	**Default:**	02:00

Setting:	**time_date.daylight_saving_amount**		
Description:	Sets the daylight savings time offset in minutes.		
Values:	0–255	**Default:**	60

Setting:	**time_date.timezone_dhcp_option**		
Description:	Enables or disables DHCP option 2/100/101 for determining time zone information.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**time_date.ntp_server_update_interval**		
Description:	Sets the delay between NTP server updates, in seconds.		
Values:	0–4294967295	**Default:**	1000

Setting:	**time_date.time_and_date**		
Description:	Manually sets the date and time. Use the format <year>-<month>-<day>T<hour>:<minute>:<second>		
Values:	<year>-<month>-<day>T <hour>:<minute>:<second>	**Default:**	2015-01-01T12:00:00

"log" Module: Log Settings

The log settings control system logging activities. System logging may be required for troubleshooting purposes. The following logging modes are supported:

- Serial/Console—system log output to an external console using a serial/RS-232 cable
- Syslog server—output to a log file on a separate server
- Volatile file

The log settings follow the format: log.[element].

All the log settings are included in the general configuration file.

Setting:	**log.syslog_enable**		
Description:	Enables or disables log output to syslog server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**log.syslog_server_address**		
Description:	Sets the syslog server IP address.		
Values:	Text string (IPv4)	**Default:**	Blank

Setting:	**log.syslog_server_port**		
Description:	Sets the syslog server port.		
Values:	1–65535	**Default:**	514

Setting:	**log.syslog_level**		
Description:	Sets the log level. The higher the level, the larger the debug output. 5—all 4—debug 3—info 2—warning 1—error 0—critical		
Values:	0–5	**Default:**	2

"remoteDir" Module: Remote Directory Settings

The remote directory settings follow the format: remoteDir.[element].

All these settings are exported when you manually export the configuration from the VSP600.

All the remote directory settings are included in the general configuration file.

Setting:	**remoteDir.ldap_enable**		
Description:	Enables or disables the VSP600 base station's access to the LDAP directory.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**remoteDir.ldap_directory_name**		
Description:	Sets the LDAP directory name.		
Values:	Text string	**Default:**	Blank

Setting:	**remoteDir.ldap_server_address**		
Description:	Sets the LDAP server IP address.		
Values:	Text string	**Default:**	Blank

Setting:	**remoteDir.ldap_port**		
Description:	Sets the LDAP server port.		
Values:	1–65535	**Default:**	389

Setting:	**remoteDir.ldap_protocol_version**		
Description:	Sets the LDAP protocol version.		
Values:	version_2, version_3	**Default:**	version_3

Setting:	**remoteDir.ldap_authentication_type**		
Description:	Sets the LDAP authentication type.		
Values:	simple, ssl	**Default:**	simple

Setting: `remoteDir.ldap_user_name`

Description: Sets the LDAP authentication user name.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_access_password`

Description: Sets the LDAP authentication password.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_base`

Description: Sets the LDAP search base. This sets where the search begins in the directory tree structure. Enter one or more attribute definitions, separated by commas (no spaces). Your directory may include attributes like "cn" (common name) or "ou" (organizational unit) or "dc" (domain component). For example, ou=accounting,dc=vtech,dc=com

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_max_hits`

Description: Sets the maximum number of entries returned for an LDAP search. Limiting the number of hits can conserve network bandwidth.

Values: 0–32000 **Default:** 200

Setting: `remoteDir.ldap_search_delay`

Description: Sets the LDAP maximum search delay in seconds.

Values: 0–500 **Default:** 0

Setting: `remoteDir.ldap_firstname_filter`

Description: Sets the LDAP first name attribute filter.

Values: Text string **Default:** Firstname

Setting: `remoteDir.ldap_lastname_filter`

Description: Sets the LDAP last name attribute filter.

Values: Text string **Default:** Lastname

Setting: `remoteDir.ldap_number_filter`

Description: Sets the LDAP number filter.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_firstname_attribute`

Description: Sets the name attributes. Enter the name attributes that you want the VSP600 to display for each entry returned after an LDAP search. Separate each attribute with a space. For example, givenName sn will display the first name and surname for each entry.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_lastname_attribute`

Description: Sets the last name attributes.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_work_number_attributes`

Description: Sets the number attributes. Enter the number attributes that you want the VSP600 to display for each entry returned after an LDAP search. Separate each attribute with a space. For example, telephoneNumber mobile will display the work phone number and mobile phone number for each entry.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_mobile_number_attributes`

Description: Sets the mobile number attributes.

Values: Text string **Default:** Blank

Setting: `remoteDir.ldap_other_number_attributes`

Description: Sets the “other” number attributes.

Values: Text string **Default:** Blank

Setting:	**remoteDir.ldap_incall_lookup_enable**
Description:	Enables or disables LDAP incoming call lookup. If enabled, the VSP600 searches the LDAP directory for the incoming call number. If the number is found, the VSP600 uses the LDAP entry for CID info.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	**remoteDir.ldap_outcall_lookup_enable**
Description:	Enables or disables LDAP outgoing call lookup. If enabled, numbers entered in pre-dial or live dial are matched against LDAP entries. If a match is found, the LDAP entry is displayed for dialing.
Values:	0 (disabled), 1 (enabled) **Default:** 0

"web" Module: Web Settings

The web settings control the web server IP, port, and security settings.

The web settings follow the format: web.[element].

All the web settings are included in the general configuration file.

Setting:	**web.http_port**		
Description:	Sets the http port when http is enabled.		
Values:	1–65535	**Default:**	80

Setting:	**web.https_enable**		
Description:	Sets server to use the https protocol.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**web.https_port**		
Description:	Sets the https port when https is enabled.		
Values:	1–65535	**Default:**	443

"user_pref" Module: User Preference Settings

The user settings are accessible to the VSP600 user. These settings are useful for initial setup. You may wish to remove these settings from auto-provisioning update files so that users do not have their own settings overwritten.

The user preference settings follow the format: user_pref.[element].

The user preference setting is included in the general configuration file.

Setting:	**`user_pref.web_language`**		
Description:	Sets the language that appears on the WebUI.		
Values:	en, fr, es	**Default:**	en

"call_settings" Module: Call Settings

The call settings configure data related to a user's call preferences. The data is stored internally at /mnt/flash/CallSettings.xml.

All the call settings (except one) follow the format: call_settings.account.x.[element] where x is an account number ranging from 1 to 6.

All the call settings are included in the MAC-specific configuration file.

Setting:	**call_settings.account.x.block_anonymous_enable**		
Description:	Enables or disables anonymous call blocking.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**call_settings.account.x.outgoing_anonymous_enable**		
Description:	Enables or disables outgoing anonymous calls.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**call_settings.account.x.dnd_enable**		
Description:	Enables or disables Do Not Disturb for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**call_settings.account.x.call_fwd_always_enable**		
Description:	Enables or disables Call Forward Always for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**call_settings.account.x.call_fwd_always_target**		
Description:	Sets the Call Forward Always target number for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**call_settings.account.x.call_fwd_busy_enable**		
Description:	Enables or disables Call Forward Busy for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**`call_settings.account.x.call_fwd_busy_target`**		
Description:	Sets the Call Forward Busy target number for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**`call_settings.account.x.cfna_enable`**		
Description:	Enables or disables Call Forward No Answer for account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**`call_settings.account.x.cfna_target`**		
Description:	Sets the Call Forward No Answer target number for account x.		
Values:	Text string	**Default:**	Blank

Setting:	**`call_settings.account.x.cfna_delay`**		
Description:	Sets the Call Forward No Answer delay (in number of rings) for account x.		
Values:	1–10	**Default:**	6

"file" Module: Imported File Settings

The "file" parameters enable the provisioning file to import additional configuration files of various types, including:

- Contact lists
- Security certificates

The following certificates are supported:

- Per-account TLS certificate (you can choose to use the Account 1 certificate for all accounts)
- LDAP
- Web server (the VSP600 has a default self-signed web server certificate)
- Provisioning
- Languages

File parameter values are URLs that direct the VSP600 to the location of the file to be imported.

None of these settings are exported when you manually export the configuration from the VSP600.

General configuration file settings

Setting: `file.https_user.certificate`

Description: URI of HTTPS server certificate to be imported; for example, <protocol>://<user>:<password>@<host>:<port>/<url-path>

Values: Text string **Default:** Blank

Setting: `file.provisioning.trusted.certificate`

Description: URI of provisioning certificate to be imported; for example, <protocol>://<user>:<password>@<host>:<port>/<url-path>

Values: Text string **Default:** Blank

Setting: `file.sips.trusted.certificate.x`

Description: URI of SIPS (TLS transport) certificate to be imported for account x; for example, <protocol>://<user>:<password>@<host>:<port>/<url-path>

Values: Text string **Default:** Blank

MAC-specific configuration file settings

Setting: `file.ldap.trusted.certificate`

Description: URI of LDAP certificate to be imported; for example, <protocol>://<user>:<password>@<host>:<port>/<url-path>

Values: Text string **Default:** Blank

Setting: `file.contact.directory.append`

Description: URL of contact directory to be imported. Entries in the imported file will be added to existing directory entries.

Values: Text string **Default:** Blank

Setting: `file.contact.directory.overwrite`

Description: URL of contact directory to be imported. Entries in the imported file will replace all existing directory entries.

Values: Text string **Default:** Blank

Setting: `file.contact.blacklist.append`

Description: URL of contact blacklist to be imported. Entries in the imported file will be added to existing blacklist entries.

Values: Text string **Default:** Blank

Setting: `file.contact.blacklist.overwrite`

Description: URL of contact blacklist to be imported. Entries in the imported file will replace all existing directory entries.

Values: Text string **Default:** Blank

"tone" Module: Tone Definition Settings

The Tone Definition settings configure data for various tones for the purpose of localization. The Audio Manager component uses the data from this model to populate the mcu on bootup.

Each tone definition must be a string of 12 elements separated by a space:

"<num of freq> <freq1> <amp1> <freq2> <amp2> <freq3> <amp3> <freq4> <amp4> <on duration> <off duration> <repeat count>"

Where:

<num of freq>: 0-4

<freq1>: 0-65535

<amp1>: -32768-32767

<freq2>: 0-65535

<amp2>: -32768-32767

<freq3>: 0-65535

<amp3>: -32768-32767

<freq4>: 0-65535

<amp4>: -32768-32767

<on duration>: 0-2^32

<off duration>: 0-2^32

<repeat count>: 0-65535

All the tone definition settings are included in the general configuration file.

Setting:	**tone.call_waiting_tone.num_of_elements**		
Description:	Sets the number of elements for the call waiting tone.		
Values:	1–5	**Default:**	1

Setting:	**tone.call_waiting_tone.element.1**		
Description:	Defines the call waiting tone element 1.		
Values:	Tone element string	**Default:**	1 440 -150 0 0 0 0 0 0 500 0 1

Setting: `tone.call_waiting_tone.element.x`

Description: Defines the call waiting tone element x.

Values: Tone element string **Default:** Blank

Setting: `tone.hold_reminder_tone.num_of_elements`

Description: Sets the number of tone elements for the hold reminder tone.

Values: 1–5 **Default:** 1

Setting: `tone.hold_reminder_tone.element.1`

Description: Defines the hold reminder tone element 1.

Values: Tone element string **Default:** 1 770 -120 0 0 0 0 0 0 300 0 1

Setting: `tone.hold_reminder_tone.element.x`

Description: Defines the hold reminder tone element x.

Values: Tone element string **Default:** Blank

Setting: `tone.inside_dial_tone.num_of_elements`

Description: Sets the number of tone elements for the dial tone.

Values: 1–5 **Default:** 1

Setting: `tone.inside_dial_tone.element.1`

Description: Defines the inside dial tone element 1.

Values: Tone element string **Default:** 2 440 -180 350 -180 0 0 0 0 4294967295 0 65535

Setting: `tone.inside_dial_tone.element.x`

Description: Defines the inside dial tone element x.

Values: Tone element string **Default:** Blank

Setting: `tone.stutter_dial_tone.num_of_elements`

Description: Sets the number of tone elements for the stutter dial tone.

Values: 1–5 **Default:** 2

Setting: `tone.stutter_dial_dial_tone.element.1`

Description: Defines the stutter dial tone element 1.

Values: Tone element string **Default:** 2 440 -180 350 -180 0 0 0 0 100 100 10

Setting: `tone.stutter_dial_dial_tone.element.2`

Description: Defines the stutter dial tone element 2.

Values: Tone element string **Default:** 2 440 -180 350 -180 0 0 0 0 4294967295 0 65535

Setting: `tone.stutter_dial_tone.element.x`

Description: Defines the stutter dial tone element x.

Values: Tone element string **Default:** Blank

Setting: `tone.busy_tone.num_of_elements`

Description: Sets the number of tone elements for the busy tone.

Values: 1–5 **Default:** 2

Setting: `tone.busy_tone.element.1`

Description: Defines the busy tone element 1.

Values: Tone element string **Default:** 2 480 -180 620 -180 0 0 0 0 500 500 65535

Setting: `tone.busy_tone.element.x`

Description: Defines the busy tone element x.

Values: Tone element string **Default:** Blank

Setting: `tone.ring_back_tone.num_of_elements`

Description: Sets the number of tone elements for the ringback tone.

Values: 1–5 **Default:** 1

Setting:	**tone.ring_back_tone.element.1**		
Description:	Defines the ringback tone element 1.		
Values:	Tone element string	**Default:**	2 440 -180 480 -180 0 0 0 0 2000 4000 65535

Setting:	**tone.ring_back_tone.element.x**		
Description:	Defines the ringback tone element x.		
Values:	Tone element string	**Default:**	Blank

"profile" Module: Password Settings

The password settings allow you to set the default administrator and user passwords in the configuration file. The administrator password is usually included in the general configuration file, while the user password is usually included in the MAC-specific configuration file. The passwords can also be set using the WebUI. Be aware that scheduled provisioning configuration file updates may reset these passwords.

General configuration file settings

Setting:	**profile.admin.access_password**		
Description:	Sets the administrator password for accessing the admin menus on the VSP601 and the WebUI.		
Values:	Text string (15 characters maximum)	**Default:**	admin

MAC-specific configuration file settings

Setting:	**profile.user.access_password**		
Description:	Sets the user password for logging on to the WebUI and editing user-accessible settings.		
Values:	Text string (15 characters maximum)	**Default:**	user

CHAPTER 6

TROUBLESHOOTING

If you have difficulty with your VSP600 base station, please try the suggestions below.

NOTE For customer service or product information, contact the person who installed your system. If your installer is unavailable, visit our website at *businessphones.vtech.com* or call **1 (888) 370-2006**.

Common Troubleshooting Procedures

Follow these procedures to resolve common issues. For more troubleshooting information, see the user's manual for your product.

The DECT handset doesn't register. "Registration failed" appears on the screen.

- Ensure the handset is fully charged and in the charger. Remove and replace the handset in its charger before selecting **Register** on the VSP600.
- Ensure the handset is not already registered to another base. If it has been registered to another base, deregister it.

The firmware upgrade or configuration update isn't working.

- Before using the WebUI, ensure you have the latest version of your web browser installed. Some menus and controls in older browsers may operate differently than described in this manual.
- Ensure you have specified the correct path to the firmware and configuration files on the **SERVICING > Firmware Upgrade > Auto Upgrade** page and the **SERVICING > Provisioning** page.
- If the phone is not downloading a MAC-specific configuration file, ensure the filename is all upper case.

Provisioning: "Use DHCP Option" is enabled, but the VSP600 is not getting a provisioning URL from the DHCP Server.

- Ensure that DHCP is enabled in Network settings.

APPENDIXES

Appendix A: Maintenance

Taking care of your products

- Your VSP600 base station contains sophisticated electronic parts, so you must treat it with care.
- Avoid rough treatment.
- Place the handset down gently.
- Save the original packing materials to protect your VSP600 base station if you ever need to ship it.

Avoid water

- You can damage your VSP600 base station if it gets wet. Do not use the handset in the rain, or handle it with wet hands.Do not install the VSP600 base station near a sink, bathtub or shower.

Electrical storms

- Electrical storms can sometimes cause power surges harmful to electronic equipment. For your own safety, take caution when using electric appliances during storms.

Cleaning your products

- Your VSP600 base station has a durable plastic casing that should retain its luster for many years. Clean it only with a soft cloth slightly dampened with water or a mild soap.
- Do not use excess water or cleaning solvents of any kind.

Remember that electrical appliances can cause serious injury if used when you are wet or standing in water. If the VSP600 base station should fall into water, DO NOT RETRIEVE IT UNTIL YOU UNPLUG THE POWER CORD AND NETWORK CABLE FROM THE WALL, then pull the unit out by the unplugged cords.

Appendix B: GPL License Information

Portions of the software associated with this product are open source, and fall within the scope of the GNU General Public License (GPL). Accordingly, those portions of code are available to the public, consistent with the requirements of the GPL, in either source code format or object code format, depending upon the nature of the code at issue. If you would like to exercise your right to receive the available code, please send a written request for the available code, along with a cashier's check, payable to VTech Communications, Inc., in the amount of $15.00 (U.S.$) to:

VTech Communications, Inc.,
9590 SW Gemini Drive, Suite 120
Beaverton OR 97008
ATTN: Information Technology Group—VSP600 GPL code request

If your request does not fully comply with the foregoing requirements, VTech reserves the right to reject your request. Further, by requesting and receiving the available code, you release VTech, its affiliates, and its and their officers, directors, employees, and representatives ("VTech Parties") from any liability or responsibility relating to such code, and you acknowledge that the VTech Parties make no representations with respect to the origin, accuracy, usability, or usefulness of such code, and the VTech Parties have no responsibility to you whatsoever concerning the code, including without limitation any responsibility to provide explanation, support, upgrade, or any communication whatsoever. Your review or use of the available code is at your sole risk and responsibility.