vtech®

ErisTerminal® SIP Deskset
VSP861
Administrator and Provisioning Manual

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 VSP861 SIP deskset with software version 2.0.4.0. See *"Using the Status menu" on page 30* for instructions on checking the software version on the VSP861. Please read this manual before installing the product.

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

Model number: VSP861

Type: Small to medium business SIP-endpoint deskset

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.
Notes provide important information about a feature or procedure.	Example of a Note.
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 VSP861 SIP deskset 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 VSP861-specific configurations for optimal performance with those services. For the latest updates, visit our website at *businessphones.vtech.com*.

Related Documents

The **VSP861 Quick Start Guide** contains a quick reference guide to the VSP861 external features and brief instructions on connecting the VSP861 to a working IP PBX system.

The **VSP861 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*.

C H A P T E R   1

INTRODUCING THE VSP861

This administrator and provisioning guide contains detailed instructions for configuring the VSP861 SIP deskset. Please read this guide before attempting to configure the VSP861.

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 VSP861 deskset" on page 10*
- *"Quick Reference Guide" on page 11*
- *"Programmable Feature Keys" on page 15*
- *"Network Requirements" on page 19*
- *"VSP861 Configuration Methods" on page 20*
- *"Adding a Custom Logo" on page 21*
- *"Using an SD card" on page 22*.

About the VSP861 deskset

The VTech VSP861 SIP deskset is a business phone designed to work with popular SIP telephone (IP PBX) equipment and services. Once you have ordered and configured your SIP equipment or service, the VSP861 enables you to make and receive calls as you would with any other business phone. The VSP861 provides calling features like hold, transfer, conferencing, speakerphone, speed-dial numbers and one-touch directory access.

The VSP861 deskset features include:

- Speakerphone, headset, hold and mute

- Up to 8 SIP account registrations

- Up to 10 active SIP sessions

- 3-way conferencing

- 30 programmable feature keys

- Message Waiting alert LED

- Dual GigE Ethernet ports

- Power over Ethernet enabled

- DECT cordless headset and cordless handset support
  For information about registering a cordless headset, see the VSP861 Deskset User's Guide. For information about registering a cordless handset, see the VSP601 Handset Quick Start Guide.

- Micro SD card slot for call recording, network traces, system logging, firmware updates and configuration file backup and updates.

- 1000-entry Call Log

There are two network ports, known as the Ethernet port and PC port, at the back of the VSP861. The Ethernet port allows the VSP861 deskset to connect to the IP PBX. The PC port is for another device such as a personal computer to connect to the Ethernet network through the VSP861.

You can configure the VSP861 using the menus on the phone, a browser-based interface called the WebUI, or an automatic provisioning process (see *"Provisioning Using Configuration Files" on page 132*). The WebUI enables you to configure the VSP861 using a computer that is connected to the same Local Area Network. The WebUI resides on the VSP861, and may get updated with firmware updates.

The VSP861 SIP deskset supports intercom and call transfers between system extensions and can connect you and two other parties on the same conference call.

The VSP861 has 30 programmable feature keys. You can program these keys for quick dial, busy lamp field, line access or any of the functions described in *"Programmable Feature Keys" on page 15*.

Quick Reference Guide

The controls you will need to use to configure the VSP861 manually are described below.

Front panel features

SD card slot (on back)

MESSAGE WAITING indicator
Flashes when you have a new voice message.

SCREEN
Displays call information, menu icons, and deskset menus.

NAVIGATION PAD
Press ▼ or ▲ to scroll through menus, highlight items or change settings.
While entering text, press ◄ or ► to move the cursor left or right.
Press **OK** to select a menu item or save a setting.

Corded headset input (on side)

MUTE
During a call, press to mute the microphone.

– VOLUME +
Press to:
• adjust the listening volume during a call.
• adjust the playback volume during message playback.
• adjust the ringer volume when the phone is idle.

HEADSET
When a headset is connected to the phone, press to make, answer or hang up a call.

CANCEL
Press to cancel an operation or exit a menu.

HOLD
Press to put a call on hold.

REDIAL
Press to view list of previously dialed numbers.

SPEAKER
Press to turn the speakerphone on or off.

MIC (underneath)

The external features that are relevant to installation and configuration are described below.

Rear panel connection ports

Ethernet/LAN port ———

Power adapter jack

PC port ———

Reserved for future use
Do not connect to other equipment.
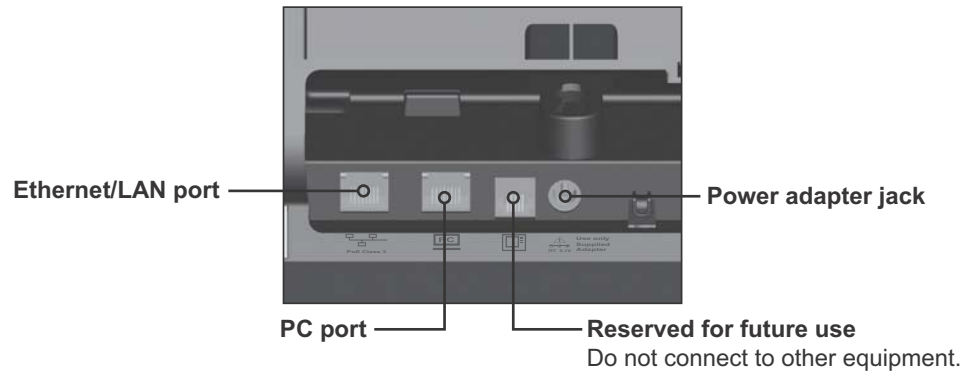
Home screen

The Home screen appears after the phone is connected and configured for your SIP PBX service. The Home screen indicates that you have no active or held calls.

If you have an active call or are viewing a menu, you can view the Home screen at any time by pressing ⌂ .

Pressing a shortcut on the Home screen opens the application associated with that shortcut.

To view additional pages of shortcuts, press ⏴ or ⏵ .

You can program and reconfigure these keys to suit your needs. See *"Configuring the Home screen shortcuts" on page 27*.
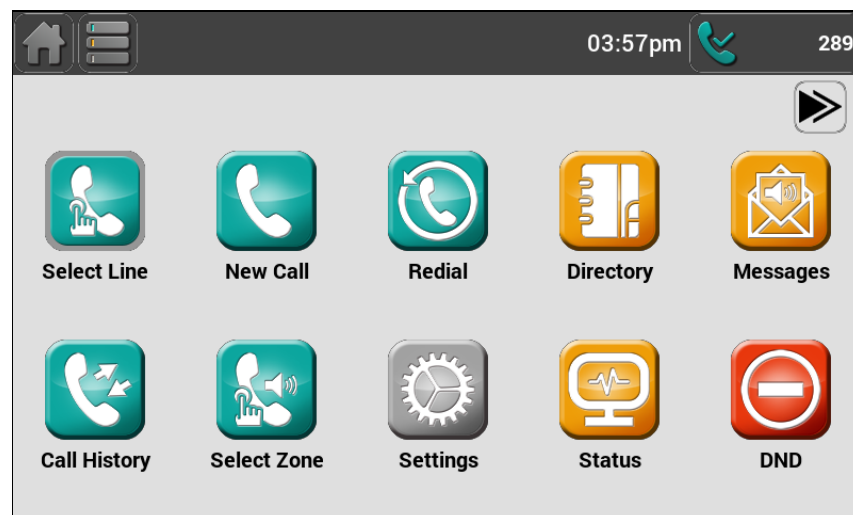
The Home screen is one of three possible default screens. The default screen appears when your phone is idle. You can select your prefered default screen on the **App Settings** menu. See *"Configuring the Default screen" on page 25*.

Your system administrator can add a custom background to the Home screen. The appearance of your Home screen and the available shortcuts may differ from that shown.

Feature Keys

The deskset offers 30 virtual feature keys that give you quick access to phone features and call functions. You can program and reconfigure these keys to suit your needs. See *"Programmable Feature Keys" on page 15* and *"Configuring the Feature keys" on page 28*.

There are 15 feature keys displayed per page.

To view additional pages of feature keys, press [◀◀] or [▶▶] .

If you have an active call or are viewing a menu, you can view the Feature Keys screen at any time by pressing [≡].
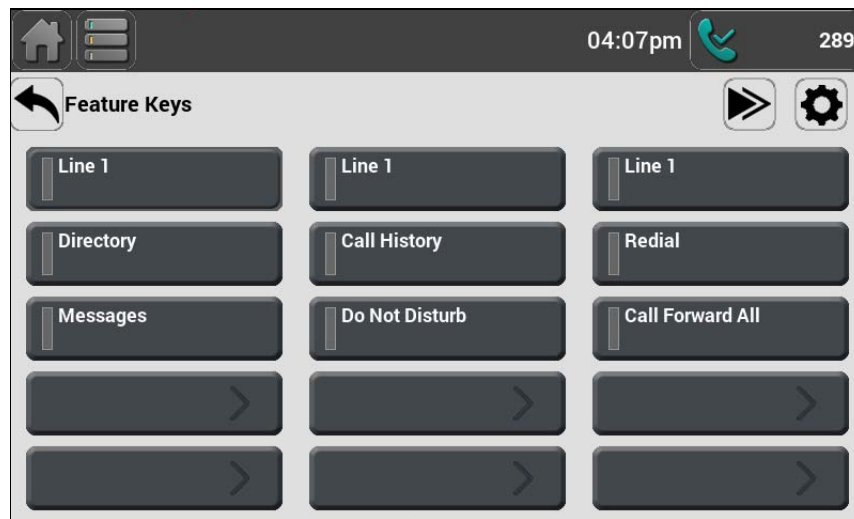
A multicolored indictor on each feature key shows you call status and other information. See *"LED Behavior" on page 18*.

Programmable Feature Keys

The table below lists the default settings for the programmable feature keys (PFKs). The key assignments on your phone may be different. Some keys may be programmed as Quick Dial keys, for example. You can assign functions to programmable keys using the

phone menu (**Settings** > **User Settings > Programmable Keys > Feature Keys**), using the WebUI, or via provisioning and the configuration file.

For more information about assigning functions to programmable keys using the phone menu, see *"Configuring the Feature keys" on page 28* and the User Guide.

To assign functions to programmable keys using the WebUI, see *"Programmable Feature Keys" on page 72*.

For the programmable key configuration file parameters, see *"pfk Module: Programmable Feature Key Settings" on page 192*.

Table 2. Programmable key default settings

Key Number	Setting
1	Line—Account 1*
2	Line—Account 1
3	Line—Account 1
4	Directory
5	Call History
6	Redial
7	Messages
8	Do Not Disturb
9	Call Forward All
10	None
11	None
12	None
13–	None

* You can assign more than one key to an account. For example, you can configure Line keys 1 and 2 to access Account 1, and Line keys 3 and 4 to access Account 2. Use the key label card to label the keys appropriately for VSP861 users after configuration.

Other possible programmable key settings

- Do Not Disturb All—Turns DND on for all registered accounts.

- Call Forward No Answer—Turns Call Forward No Answer (CFNA) on and off. When CFNA is on, unanswered incoming calls are forwarded to another number after a specified delay.

- Call Forward Busy—Turns Call Forward Busy (CFB) on and off. When CFB is on, incoming calls are forwarded to another number when the line is busy.

- Quick Dial

- BLF—Busy lamp field keys let you monitor activity at other phones. The key LED indicates call status.

- Page—If this feature is enabled, press the Page key to call one or a group of phones. You can configure pages to be automatically answered. See *"SIP Account Management" on page 51*.

- Multicast page—Press the Multicast page key to page all phones in a pre-defined paging zone. See *"Paging Zones" on page 79*.

- Park Call—Dials the access code to park your current call. To program access codes, see *"SIP Account Management" on page 51*.

- Retrieve Parked Call—Dials the access code to retrieve a parked call.

- In Call DTMF—Dials a string of numbers while you are on a call. For example, pressing the key might dial a conference access code.

- Call Return—Dials the number of the last missed call.

- Group Call Pickup—Dials the Group Call Pickup code, allowing you to answer a call ringing at any extension within an admin-defined group.

- Direct Call Pickup—Dials the Direct Call Pickup code, allowing you to answer a call ringing at a specific extension. After pressing the button, you may need to enter the extension number manually.

- Prefix Dialing—Automatically goes off-hook and dials a prefix (hidden from the user).

- Call Handling Profile—For Comverse server-side feature contol. Dials the call handling profile code along with the profile index number to activate the profile.

- Hunt Group—Dials the hunt group extension number.

- Secretarial Filtering—Turns Comverse secretarial filtering on or off.

- Phone Lock—Locks the phone or enables the user to unlock the phone with a PIN. See the phone lock section.

- Flash—Performs a hook flash, as defined in *"Programmable Feature Keys" on page 72*.

■   XML App—Displays a user-initiated (pulled) XML-based screen or menu.

LED Behavior

The programmable feature keys have LEDs that indicate various states.

Table 3. VSP861 LED behavior

Key function	LED Activity	Description
Account	Flashing ORANGE Steady GREEN Quickly flashing GREEN Slowly flashing GREEN	Account not registered Dialing or on a call Ringing incoming call Held call
Shared account	Steady ORANGE Slowly flashing ORANGE	Shared account is on a call Shared account is on hold
Do Not Disturb	Off Steady ORANGE	DND is off DND or DND All is on
Do Not Disturb All	Off Flashing ORANGE Steady ORANGE	DND is off for all lines DND is on for some lines DND All is on
Call Forward	Off Steady ORANGE	Call forwarding is off Call forwarding is on
Page	Steady GREEN	Outgoing page in progress
Busy Lamp Field	Off Steady ORANGE Quickly flashing ORANGE Blinking ORANGE	Monitored phone is idle Monitored phone is on a call The monitored phone is ringing or has a held call* BLF registration error *Held call indication applies only to certain servers.
Call Handling Profile	Off Steady Orange	No CHP activated CHP activated
Secretarial Filtering	Off Steady ORANGE	Secretarial Filtering is off Secretarial Filtering is on
Hunt Group	Off Steady ORANGE	Hunt Group is off Hunt Group is on

Network Requirements

A simple VSP861 SIP deskset installation example is shown in Figure 1. A switched network topology is recommended for your LAN.

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

The VSP861 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 VSP861 desksets so that IP addresses can be auto-assigned. In most cases, your network router will have a DHCP server. By default, the VSP861 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 VSP861. You can assign a static IP address using the VSP861 menu. Go to **Admin settings > Network setting > IPv4** or **IPv6 > Static** (from the list). 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 VSP861 firmware and/or configuration settings manually.
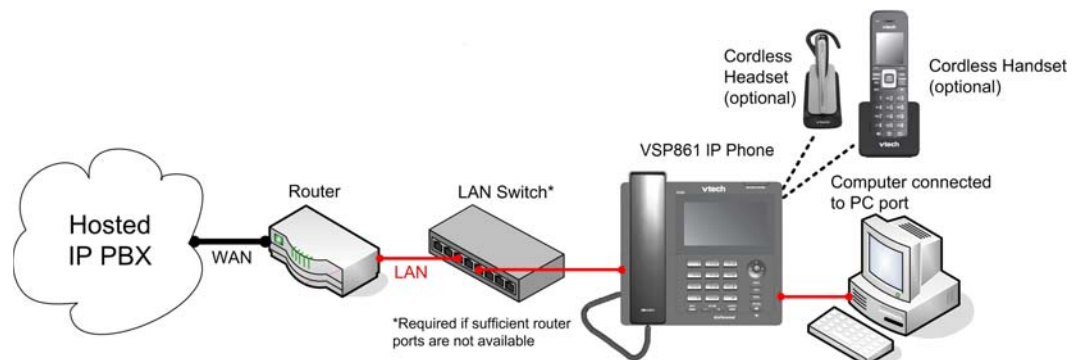
Figure 1. VSP861 Installation Example

VSP861 Configuration Methods

You can configure the VSP861 using one of the following methods:

- From the VSP861 itself, using the menus. The VSP861 menus are best suited to configuring a few settings, perhaps after the initial setup has been done. For administrators, the settings available on the VSP861 menus include network settings, account settings, and provisioning settings. See *"Using the Admin Settings Menu" on page 33*. Many of the settings accessible on the VSP861 are most useful for end users. Through the menu, they can customize the screen appearance, sounds, and manage calls. For more information, see the VSP861 User Guide.

- The Web User Interface, or WebUI, which you access using your Internet browser. See *"Using the WebUI" on page 45*. The browser-based interface is easy to navigate and best suited to configuring a large number of VSP861 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, configure the programmable keys, and set up provisioning, which will allow you to automatically and remotely update the VSP861 after initial configuration.

- Provisioning using configuration files. Working with configuration files is the best way to configure multiple phones. There are several methods available to enable the VSP861 to locate and upload the configuration file. For example, you can enable the VSP861, 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 VSP861 automatically downloads the file and applies the new settings. For more information, see *"Provisioning Using Configuration Files" on page 132*.

Adding a Custom Logo

You can upload a custom logo to be displayed on the phone idle screen and during bootup. Uploading a logo is done using the WebUI or the configuration file. For WebUI configuration, see *"Custom Image/Logo" on page 111*. The configuration file parameters for uploading a custom logo are described in *"Uploading a custom logo" on page 21*. The default logo for bootup and idle mode is the **vtech** logo.

Logo specifications

The file type and dimensions for the logo are listed below.

File type: 24-bit colour (.bmp, .jpg, or .png)

Dimensions (w × h): Idle screenlogo: 800x480 pixels

Positioning a custom logo on the screen is a matter of creating a logo with the maximum dimensions listed above, including any surrounding white space. There are no configuration file settings to specify the x-axis or y-axis position of the logo on the screen.

Uploading a custom logo

The file.bootup_logo and file.idle_logo parameters in the configuration file allow you to upload a custom bootup logo and custom idle logo. Place the logos on your server and enter the URL for each logo for the file.idle_logo and file.bootup_logo parameters.

If the downloaded logo is found to be invalid, the syslog will record one of the following errors:

- file not found

- invalid file format

- incorrect image size

Using an SD card

The micro SD card slot on the back of the VSP861 provides the following feature:

■ Local call recording—allows the user to record a two-way conversation during a call. The recording is stored in the available memory of the SD card.

You can configure local call recording on the desket menu, WebUI, and configuration file. See *"Using the Call Recording menu" on page 40* and *"Local Call Recording" on page 86*.

You can view the SD card memory usage on the SD card menu (available on the deskset User settings menu) or on the WebUI status page (see *"Status Page" on page 49*).

Inserting and ejecting an SD card

The deskset will detect the SD card upon insertion. A splash screen indicating detection will appear for two seconds.

To eject the SD card:

1. When the VSP861 is idle, press **Settings** on the Home screen.

2. Press **User settings**.

3. On the Settings menu, scroll down and press **Storage**.

4. On the **SD card** menu, press **Eject** .

5. Wait for the message **It is now safe to eject your SD card**, and then press down on the SD card to release it.

C H A P T E R 2

CONFIGURATION USING THE PHONE MENUS

The VSP861 **Settings** [icon] application shortcut has the following menus:

■ Call Settings—set DND, call forward settings, message settings, block anonymous numbers, dial anonymous, set call waiting/missed call alerts, and enable auto answer.

■ App Settings—delete call history, set default screen, sort/delete directory and blacklist entries, and selecting applications to be displayed on the Home screen.

■ User Settings—allows the user to set the language for the display, configure the appearance of the display, edit programmable keys, register a DECT headset and customize the audio settings.

■ Admin settings—configure network settings (enter static IP addresses, for example), account settings, provisioning, security, and call recording.

This chapter contains instructions for using the Admin Settings menu and for accessing the Status menu. See the VSP861 User Guide for more information about the other menus.

Viewing the Home screen

To use the VSP861 Home screen:

1. When the VSP861 is idle, press ◀ or ▶ to display the desired Home screen page.

2. Press the button for the application shortcut you want

    (for example, ⚙).

    ■   Press **CANCEL** or ↰ to cancel an operation, exit the menu display or return to the idle screen.

    ■   Press 🏠 to return to the Home screen.

Configuring the Default screen

You can set the screen that appears when your phone is idle. Depending on your preference, you can set the screen to the Home screen (showing all the application shortcuts), the Feature keys, or the Call Manager.
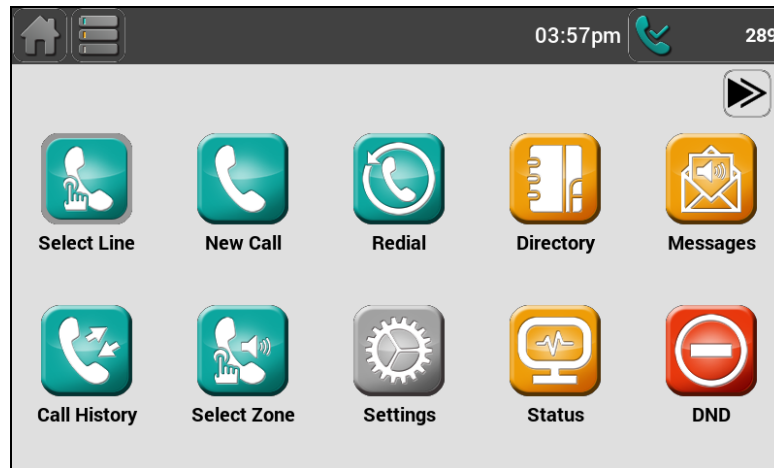
Home Screen
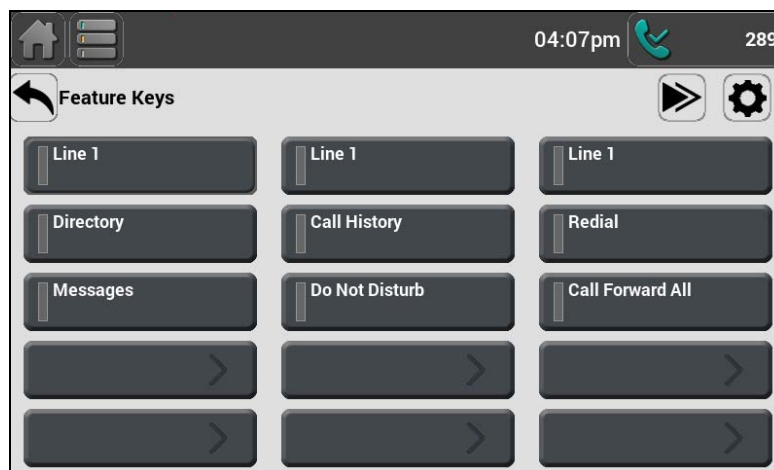
Feature Keys
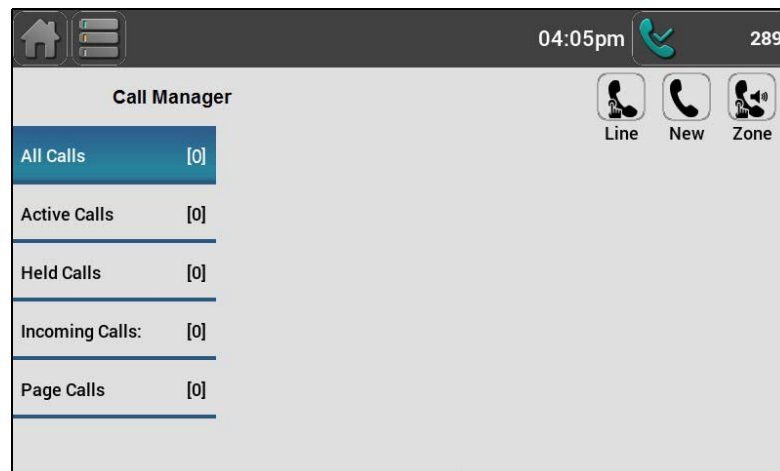
Call Manager

To configure the default screen:

1. When the VSP861 is idle, press **Settings** on the Home screen.

2. Press **App Settings.**

3. From the **Settings** menu, press **Default Screen**.

4. Select the desired default screen from the list.
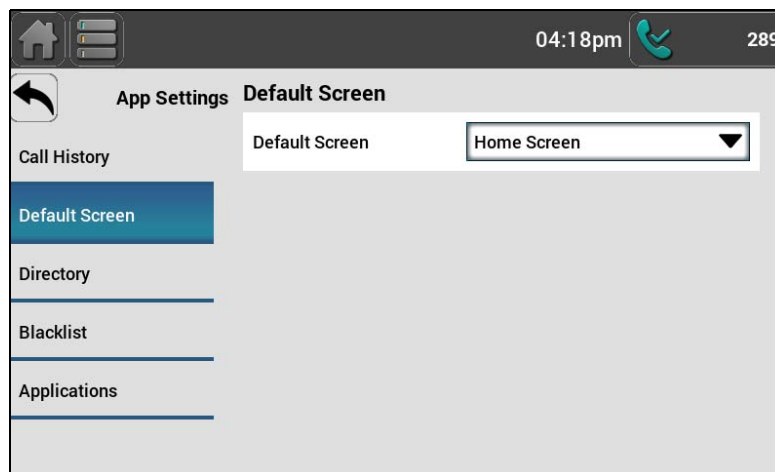
Configuring the Home screen shortcuts

You can select and arrange the shortcuts that appear on the Home screen. The Home screen can consist of three pages, with up to 10 shortcuts per page.

To configure Home screen shortcuts:

1. When the VSP861 is idle, press **Settings** on the Home screen.

2. Press **App Settings.**

3. From the **Settings** menu, press **Applications**.

   The App Settings menu appears.
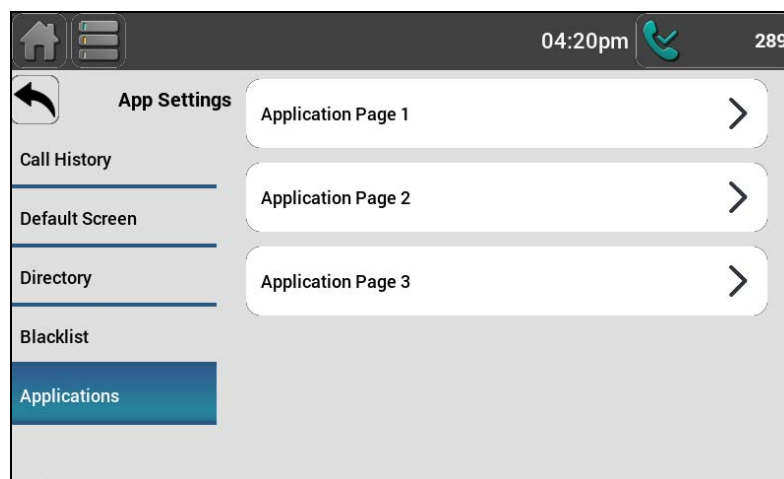
4. On the App Settings menu, select the desired Home screen page.

   A list of 10 shortcuts for the selected page appears (numbered 1 to 10 for Application page 1, 11 to 20 for Application page 2, and 21 to 30 for Application page 3).
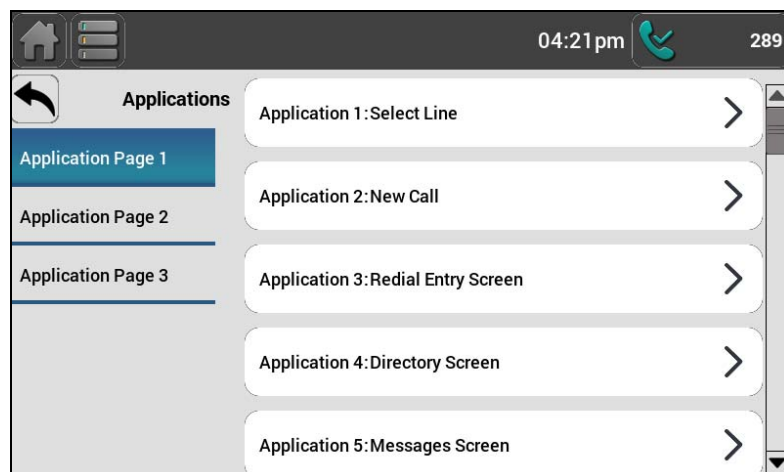
5. Select the numbered shortcut/application you would like to change or add (empty slots are labeled "Unassigned").

The menu for that application appears.
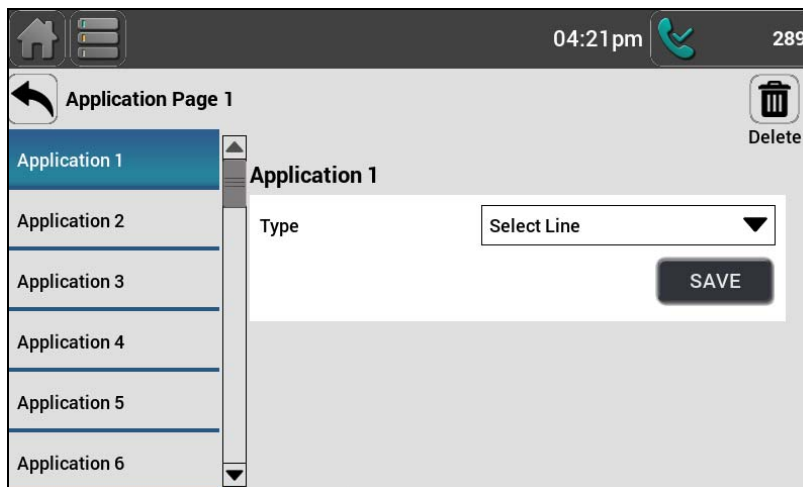
6. Select the desired shortcut from the list and then press **SAVE**.

Configuring the Feature keys

You can configure the Feature keys on the Deskset. You can also configure these keys on the WebUI (see *"Programmable Feature Keys" on page 72*).

To configure the Feature keys:

1. When the VSP861 is idle, press **Settings** on the Home screen.

2. Press **User Settings**.

3. From the User Settings menu, press **Feature Keys**.

The User Settings menu appears.
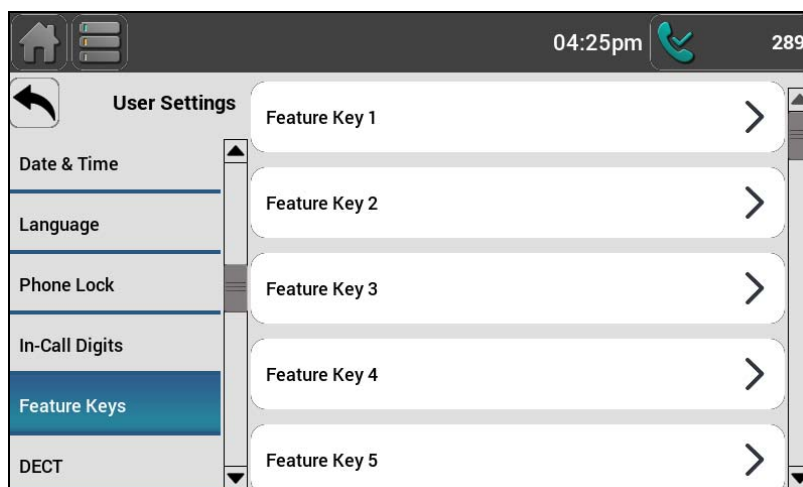
4. Select the feature key to configure.

The Feature Keys menu appears.

5. Select a feature key **Type.**

    Depending on the PFK type, the screen may prompt you to configure additional settings. For more information, see *"Programmable Feature Keys" on page 72*.

6. Enter a **Label** for the feature key.

7. Press **Save**.

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 VSP861 on the **Product Info** screen, available from the **Status** menu.

To view the Status menu:

1. When the VSP861 is idle, press **Status** on the Home screen.

    The **Status** menu appears.
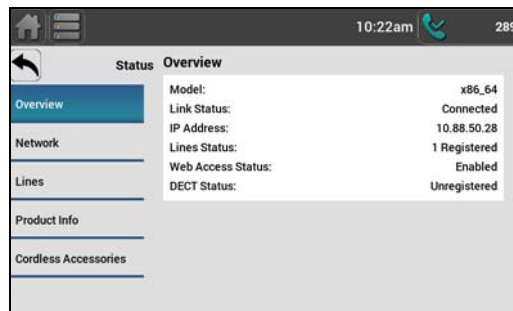
2. Press the desired menu.

The available status menus are listed in Table 4.

Table 4. Status menu summary

Menu	Information listed
1. Network (IPv4 or IPv6)	■ IP type
	■ IP address
	■ Subnet Mask
	■ Prefix (IPv6 only)
	■ Gateway IP address
	■ DNS server 1 IP address
	■ DNS server 2 IP address
	■ VPN status

Table 4. Status menu summary

Menu	Information listed
2. Lines	Lines and registration status. On the **Line** menu, select the desired line to view detailed line status information:
	■ Line status (Registered/Not registered)
	■ Account display name
	■ Account User ID
	■ Registrar Server IP address
	■ Registrar Server port number
	■ Proxy server IP address
	■ Proxy server port number
3. Product Info	■ Model number
	■ Serial number
	■ MAC address
	■ Boot version
	■ Firmware version
	■ V-Series
	■ Hardware version
	■ EMC version
	■ NTP server
4. Cordless Accessories	■ DECT handset (Registered/Not registered)
	■ DECT headset (Registered/Not registered)

Viewing Line status

To view line status, from the **Status** menu, select **Lines**. The **Lines** menu lists the available lines, along with each line's current registration status – registered, unregistered, or disabled.

To view complete status information for a line:

- On the **Lines** menu, press the desired line. The full line status screen appears.

Using the Admin Settings Menu

To access the Admin Settings menu:

1. When the VSP861 is idle, press **Settings** on the Home screen.

2. Press **Admin settings**.

3. Use the dial pad to enter the admin password, and then press ▮ **Enter** ▮ . The default password is **admin** .

The Admin settings are listed in Table 5.

Table 5. Admin setting summary

Setting	Options
Network setting See *page 35*	1. IPv4 2. IPv6 3. VLAN
Line See *page 38*	1. LINE 1 2. LINE 2 3. LINE 3 4. LINE 4 5. LINE 5 6. LINE 6 7. LINE 7 8. LINE 8
Provisioning See *page 39*	1. Server URL 2. Auth Name 3. Auth Password
Call Recording See *page 40*	1. Call Recording (Enabled, Disabled) 2. Record Tone (Enabled, Disabled)
Phone Lock See *page 41*	Restriction Mode
Remote Acccess See *page 42*	Enable Web Access

Table 5. Admin setting summary

Setting	Options
Edit password See *page 43*	1. User PW 2. Admin PW
RESET	Press to display a screen that allows you to reset the phone to factory default settings.
RESTART	Press to display a screen that allows you to restart the phone.

Using the Network menu

Use the Network menu to configure network-related settings for the VSP861. For more information about these settings, see *"Basic Network Settings" on page 88* and *"Advanced Network Settings" on page 90*.

To use the Network menu:

1. From the **Admin Settings** menu, press **Network**.
   The **Network** menu appears.
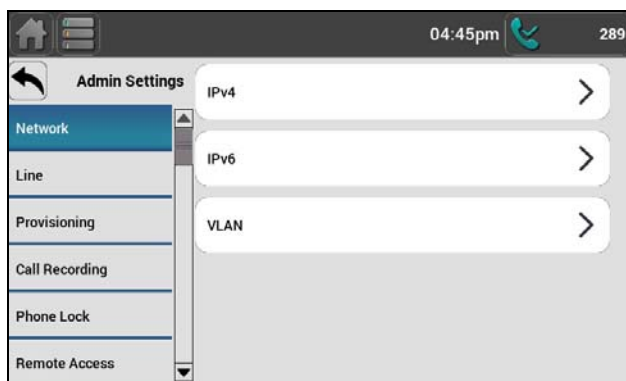
2. Press the desired option:

   ■ IPv4

   ● Mode (DHCP, Static IP, PPPoE, Disable)

   ● Enable Static DNS

   ● Primary DNS

   ● Secondary DNS

   ■ IPv6

   ● Mode (Automatic, Static, Disable)

   ● Enable Static DNS

   ● Primary DNS

   ● Secondary DNS

   ■ VLAN ID

To set the network mode:

1. From the **Network** menu, press your network type (**IPv4** or **IPv6**).
   The selected network type screen appears (**IPv4** menu shown below).
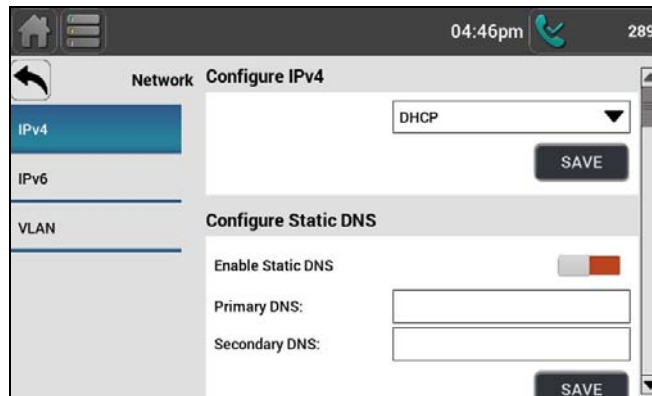
2. Select the network mode for your network type from the list, and then press **Save** .

DHCP (IPv4) or Automatic (IPv6) is enabled by default, which means the VSP861 will get its IP address from the network. When DHCP and Automatic are disabled, you must enter a static IP address for the VSP861.

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

To set static IP for the VSP861:

1. From the **Network** menu, press your network type (**IPv4** or **IPv6**), and then select **Static** from the list.

2. Enter the static **IP Address**. Use the dial pad to enter characters.

3. Enter the static **Subnet Mask**.

4. Enter the static **Gateway**.

5. Enter the IP address of the **Primary DNS** server.

6. Enter the IP address of the **Secondary DNS** server. The VSP861 uses this server if the primary server does not respond.

7. Press **SAVE** .

To set static DNS:

1. From the **Network** menu, press **IPv4** or **IPv6** .

2. Select **Static** from the list.

3. Touch the **Enable Static DNS** slider to turn it on .

4.   Enter the IP address for the **Primary DNS** server.

5.   Enter the IP address for the **Secondary DNS** server.

6.   Press ▐ **SAVE** ▐ .

To set PPPoE:

1.   From the **Network** menu, press **IPv4**

2.   Select **PPPoE** from the list.

3.   Enter the **Authentication Name**.

4.   Enter the **Authentication Password**.

5.   Press ▐ **SAVE** ▐.

To set the VLAN ID for the VSP861:

1.   From the **Network** menu, press **VLAN ID**.

2.   .Touch the **Enable WAN VLAN** slider to enable ▬▬▭ WAN VLan.

3.   Enter the WAN **VLAN ID**. The valid range is 0 to 4095.

4.   Press ▐ **SAVE** ▐.

5.   Touch the **Enable PC VLAN** slider to enable ▬▬▭ PC VLan.

6.   Enter the PC **VLAN ID**. The valid range is 0 to 4095.

7.   Press ▐ **SAVE** ▐.

Using the Line menu

Use the **Line** menu to configure line-specific settings for the phone.

To use the Line setting menu:

1. From the **Admin Settings** menu, press **Line**
    The full configuration menu for that line appears.

You can configure:

- Account label
- Display name
- User Identifier
- Authentication Name
- Authentication Password
- SIP Registrar Address
- SIP Registrar port
- SIP Proxy Address
- SIP Proxy port
- Enable Line
- Answer page automatically

For more information about these settings, see *"SIP Account Management" on page 51*.

2. Edit the Line settings using the dial pad and the buttons available for each setting:

- ◀x —deletes a character
- **123**—enables you to enter numbers, lower case letters, or upper case letters using the dial pad.
- **Save** —saves and applies the new settings

Using the Provisioning menu

Use the Provisioning menu to configure auto-provisioning settings. For more information about auto-provisioning, see *"Provisioning" on page 114* and *"Provisioning Using Configuration Files" on page 132*.

On the Provisioning menu you can configure:

- Server URL—the URL of the provisioning server. The URL can include a complete path to the configuration file.

- Auth Name—the username the VSP861 will use to access the provisioning server.

- Auth Password—the password the VSP861 will use to access the provisioning server.

To use the Provisioning menu:

1. From the **Admin Settings** menu, press **Provisioning**.
   The **Provisioning** menu appears.

2. Enter the server URL using the dial pad keys:

- ◀**x** —deletes a character

- **ABC** —enables you to enter numbers, lower case letters, or upper case letters with the dial pad.

- **Save** —prompts you to reboot the phone and apply the new settings

   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. Enter the Auth Name for access to the provisioning server if it is not part of the server string.

4. Enter the Auth Password.

5. Press **SAVE** .

Using the Call Recording menu

You can configure the call recording feature on the Call Recording menu. On the Call Recording menu you can enable and disable:

- call recording
- the call record tone (played over the line when recording begins and ends).

> **NOTE**
> If you attempt to enable Call Recording with no SD card inserted, the deskset displays a **No SD card detected.** message.

To use the Call Recording menu:

1. From the **Admin Settings** menu, press **Call Recording**.
   The **Call Recording** menu appears.
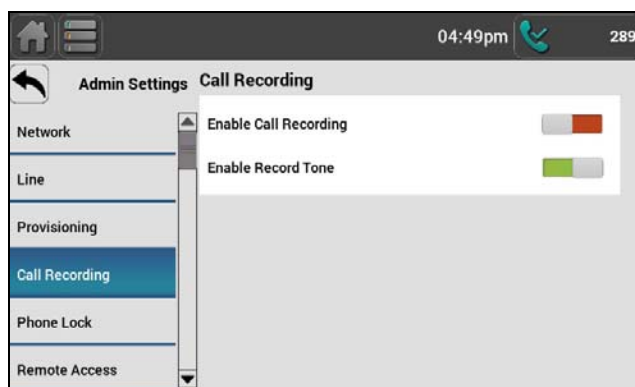
2. Touch the **Enable Call Recording** slider to enable or disable Call Recording.

3. Touch the **Enable Record Tone** slider to enable or disable the Record Tone.

4. Press .

Using the Phone Lock menu

On the Phone Lock menu, you can configure the phone lock feature. The Phone Lock feature restricts certain hard keys and features unless the user enters a PIN code.

Emergency Call Only locks out all outgoing calls except emergency calls. Emergency numbers must match the Emergency Dial Plan, as configured under *"General Account Settings" on page 51*. Incoming calls are still allowed.

To use the Phone Lock menu:

1. From the **Admin Settings** menu, press **Phone Lock**.
    The **Usage Restriction** menu appears.
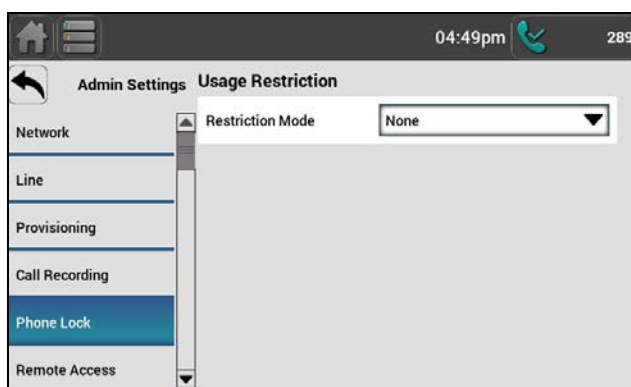
2. Select a **Restriction Mode** from the list.

    ■   None

    ■   Emergency Call Only

3. Press ⬑.

Using the Remote Access menu

On the Remote Access menu, you can enable or disable the Web server. The Web server setting determines whether the embedded WebUI is available from the phone. When the Web server is disabled, the phone can be configured using the phone menus or via provisioning only.

To use the Remote Access menu:

1. From the **Admin Settings** menu, press **Remote Access**.
   The **Web Access** menu appears.
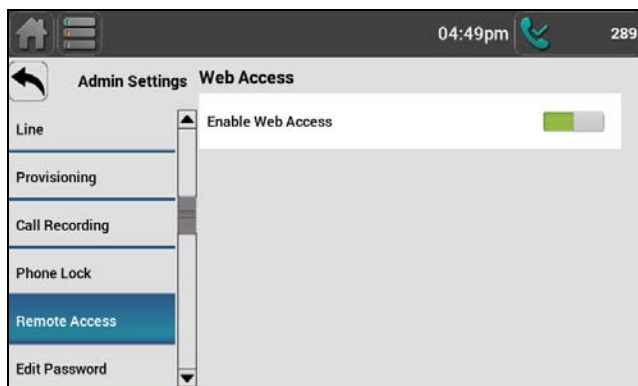
2. Touch the **Enable Static DNS** slider to enable [green] or disable [red] WebUI access to the phone.

3. Press [back arrow].

Using the Edit Password menu

On the Edit password menu, you can reset the current User and Admin passwords.

> **NOTE** By default, after bootup, the phone alerts you if the default passwords (user password and admin password) are still in use.

To reset the User password:

1. From the **Admin Settings** menu, press **Edit Password**.
    The following menu appears.
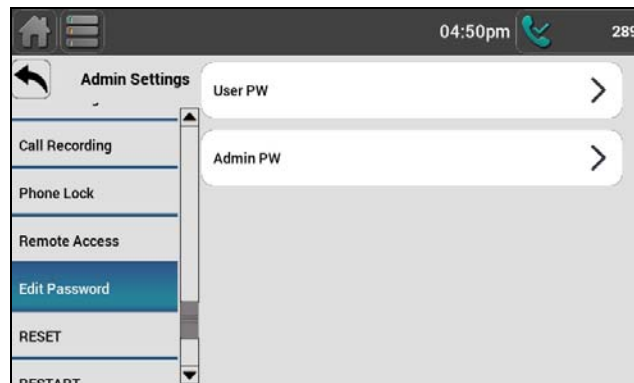
2. Press **User PW**.
    The Edit Password screen appears.
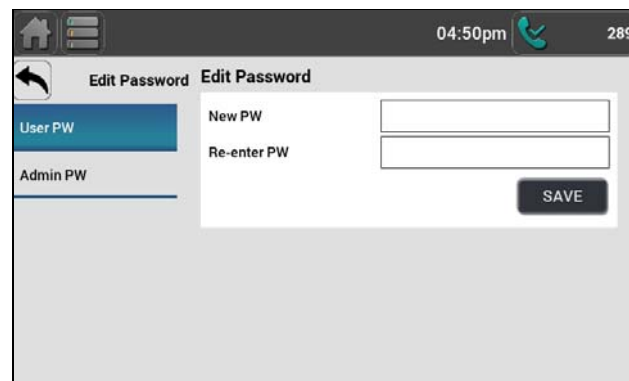
3. Enter the new password using the dial pad keys.

4. Re-enter the new password.

5. Press ▮ **Save** ▮.

To reset the User password:

1. From the **Admin Settings** menu, press **Edit Password**.
    The following menu appears.
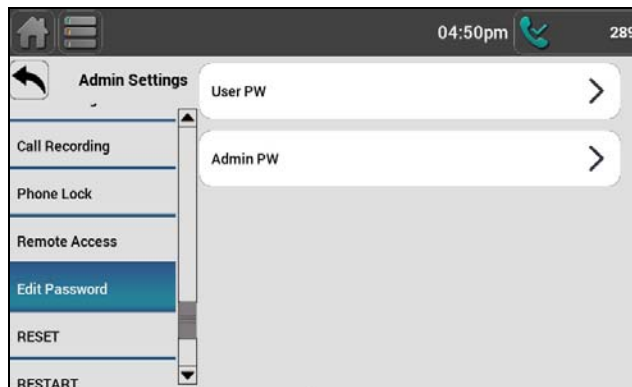
2. Press **Admin PW**.
   The Edit Password screen appears.
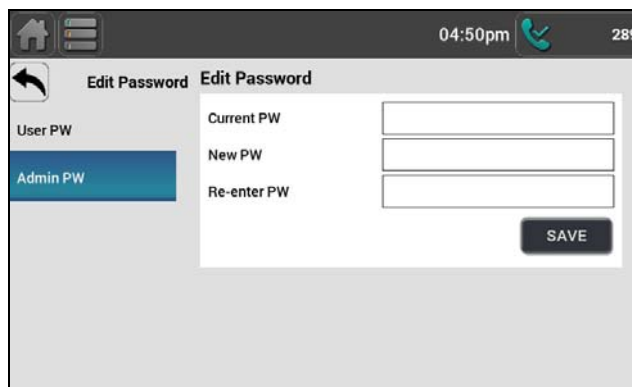
3. Enter the current password using the dial pad keys.

4. Enter the new password.

5. Re-enter the new password.

6. Press   **Save** .

C H A P T E R   3

USING THE WEBUI

The WebUI allows you to configure account settings, programmable keys, network settings, contact lists, and provisioning settings. The WebUI is embedded in the VSP861 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 VSP861 settings. This chapter covers:

- *"Using the Web User Interface (WebUI)" on page 46*

- *"Status Page" on page 49*

- *"System Pages" on page 51*

- *"Network Pages" on page 87*

- *"Contacts Pages" on page 93*

- *"Servicing Pages" on page 106*.

Using the Web User Interface (WebUI)

The Web User Interface (WebUI) resides on the VSP861 deskset. You can access it using an Internet browser. After you log in to the WebUI, you can configure the VSP861 on the following pages:

System

- SIP Account Management (see *page 51*)
- Call Settings (see *page 65*)
- User Preferences (see *page 69*)
- Programmable Keys (see *page 72*)
- Speed Dial (see *page 77*)
- Ringer Settings (see *page 78*)
- Paging Zones (see *page 79*)
- Server Application (see *page 81*)
- Hotline Settings (see *page 85*)
- Local Call Recording (see *page 86*)

Network

- Basic Network Settings (see *page 88*)
- Advanced Network Settings (see *page 90*)

Contacts

- Local Directory (see *page 93*)
- Blacklist (see *page 96*)
- LDAP (see *page 99*)
- Broadsoft (see *page 102*)
- Remote XML (see *page 103*)
- Call History (see *page 105*)

Servicing

- Reboot (see *page 106*)
- Time and Date (see *page 107*)
- Custom Language (see *page 110*)
- Firmware Upgrade (see *page 112*)
- Provisioning (see *page 114*)
- Security (see *page 121*)
- Trusted Servers (see *page 125*)
- Trusted IP (see *page 126*)
- Certificates (see *page 127*)
- TR-069 (see *page 129*)
- System Logs (see *page 130*)

The WebUI also has a **System Status** page, where you can view network status and general information about the VSP861. The information on the Status page matches the **Status** menu available on the VSP861.

To access the WebUI:

1. Ensure that your computer is connected to the same network as the VSP861. Your computer may already be connected to the network through the PC port on the back of the VSP861.

2. Find the IP address of the VSP861:

    a. When the VSP861 is idle, press **Status** on the Home screen.

    b. On the Overview screen, note the IP Address.
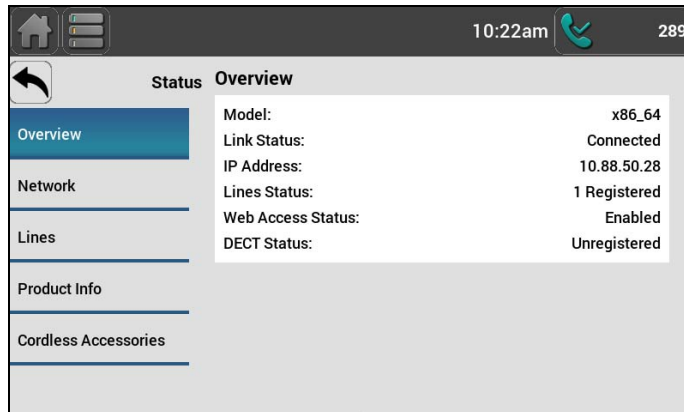
3. On your computer, open an Internet browser. (Depending on your browser, some of the pages presented here may look different and have different controls. Ensure that you are running the latest update of your preferred browser.)

4. Type the VSP861 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**.

> **NOTE**
> As a security measure, the WebUI prevents you from logging in for five minutes after four (or three, depending on the browser's cache) consecutive failed log-in attempts during a five-minute period.

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.

The settings tables in this section contain settings that appear in the WebUI, along with 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 132*.

Status Page

The WebUI System Status page is equivalent to the **Status** menu on the VSP861.

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

- **IPv4** and **IPv6** network information regarding your device's network address and network connection

- **Cordless Status** indicates whether a cordless headset and/or handset is registered to the phone.

STATUS

System Status

| STATUS | SYSTEM | NETWORK | CONTACTS | SERVICING |

General

Model:	VSP861
Serial Number:	B2300002438
MAC Address:	14:AE:DB:1B:4E:E0
Link Status:	Connected
Boot Version:	1.15
Software Version:	2.0.5.x
V-Series:	2.0.5.x
Hardware Version:	HW1.x
EMC Version:	0
Network Time Settings:	us.pool.ntp.org

Account Status

Account 1:	Registered
Account 2:	Registered
Account 3:	Registered
Account 4:	Registered
Account 5:	Not Registered
Account 6:	Not Registered
Account 7:	Not Registered
Account 8:	Not Registered

IPv4

IP Mode:	dhcp
IP Address:	10.88.50.23
Subnet Mask:	255.255.0.0
Gateway:	10.88.3.149
Primary DNS:	10.88.162.10
Secondary DNS:	10.88.162.6
VPN:	Disabled

IPv6

IP Mode:	disable
IP Address:	::
Prefix:	0
Gateway:	ff02::1
Primary DNS:	
Secondary DNS:	

Cordless Status

Headset:	Not Registered
Handset:	Not Registered

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 141*.

General Account Settings

Click the link for each setting to see the matching configuration file parameter in *"Configuration File Parameter Guide" on page 140*. 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 VSP861 display when account x is selected.
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. If the Account Label is blank, the Display Name appears on the VSP861 display when account x is selected.

Setting	Description
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.
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 54*.
Call Restriction Dial Plan	Enter a call restriction dial plan, which prevents users from completing calls that match this dial plan on this account.
Emergency Dial Plan	Enter the Emergency Dial plan, which will apply to both restricted calls (when the phone lock feature is set to Emergency Call Only—see *"Using the Phone Lock menu" on page 41* and *"Security" on page 121*) and other calls when the Phone Lock feature is not in use.
Inter Digit Timeout (secs)	Sets how long the VSP861 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.
Page Auto Answer	When set to Auto, enables the VSP861 to automatically answer when a page is received. This is usually the desired behavior for paging.
Feature Synchronization	Enables the VSP861 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 VSP861 menu and WebUI. Similarly, changes made using the VSP861 or WebUI will update the settings on the server.
Line Type	Select the line type to Private or Shared. A private line will be accessible only at the VSP861 you are configuring. Shared lines can be assigned to more than one VSP861. For more information about using shared lines, see the VSP861 User Guide.
Barge-in	Enables subscribers to shared lines to "barge in" on active calls on other shared lines.

Setting	Description
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 VSP861, disable this setting.
Call Rejection Response Code	Select the response code for call rejection. This code applies to the following call rejection cases: ■ User presses **Reject** for an incoming call (except when Call Forward Busy is enabled) ■ 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

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 VSP861 should dial the number.

There are three different types of dial plans available: general, Call Restriction, and Emergency.

In the case of overlapping dial plan definitions between Emergency, Call Restriction, and the general dial plan, the following priority (high to low) applies:

1. Emergency

2. Call Restriction

3. General

For example, in order to prevent a user from dialing extensions in the 9xx range while having 911 as the emergency number, use the following dial plans:

- Emergency dial plan = 911

- Call Restriction dial plan = 9xx

- General dial plan = xxx

A user who dials 920 will be unable to complete the call, and the message **920 is a restricted number** will appear on the phone screen. A user who dials 911 will complete an emergency dial.

> **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 51*).

Element	Description
(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.

See also .

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.

Caller Identity Settings

Setting	Description
Source Priority 1	Select the desired caller ID source to be displayed on the incoming call screen: "From" field, RPID (Remote-Party ID) or PAI (P-Asserted Identity) header.
Source Priority 2	Select the lower-priority caller ID source.
Source Priority 3	Select the lowest-priority caller ID source.

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.

Setting	Description
Codec priority 5	Select the codec to be used fifth during a call if the previous codec fails.
Codec priority 6	Select the codec to be used sixth during a call if the previous codec fails.
Codec priority 7	Select the codec to be used last 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.
DTMF Payload Type	Set the DTMF payload type for in-call DTMF from 96–127.

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 (signaling)	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: ■ UDP (User Datagram Protocol) is generally less prone to latency, but SIP data may be subject to network congestion. ■ TCP (Transmission Control Protocol) is the most reliable protocol and includes error checking and delivery validation. ■ TLS (Transport Layer Security)—the VSP861 supports secured SIP signaling via TLS. Optional server authentication is supported via user-uploaded certificates. TLS certificates are uploaded using the configuration file. See *"file Module: Imported File Parameters" on page 201* and consult your service provider.

Voice

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.

Feature Access Codes

Paging:	
Call Park:	
Parked Call Retrieval:	
Voicemail:	
DND ON:	
DND OFF:	
Call Forward All ON:	
Call Forward All OFF:	
Call Forward No Answer ON:	
Call Forward No Answer OFF:	
Call Forward Busy ON:	
Call Forward Busy OFF:	
Anonymous Call Reject ON:	
Anonymous Call Reject OFF:	
Anonymous Call ON:	
Anonymous Call OFF:	
Call Waiting ON:	
Call Waiting OFF:	
Group Call Pickup:	
Direct Call Pick Up:	
Hunt Group Sign ON:	
Hunt Group Sign OFF:	
Secretarial Filtering ON:	
Secretarial Filtering OFF:	

Feature Access Codes Settings

If your IP PBX service provider uses feature access codes, then enter the applicable codes here. You can assign many of these features to programmable feature keys, which enables end users to press the keys to dial out the codes you enter here. To configure programmable feature keys, see *"Programmable Feature Keys" on page 72*.

Setting	Description	Assignable to PFK?
Paging	Enter the paging access code.	Yes
Call Park	Enter the call park access code. Broadsoft provides a feature access code for the park feature. Asterisk/Metaswitch provides a parking lot extension number for the park feature. Enter the parking lot extension number here.	Yes

Setting	Description	Assignable to PFK?
Parked Call Retrieval	Enter the call park retrieval access code. Broadsoft and Asterisk/Metaswitch provide a feature access code for park retrieval.	Yes
Voicemail	Enter the voicemail access code. The code is dialed when the user selects a line from the phone's Message menu.	Yes
DND ON	Enter the Do Not Disturb ON access code.	Yes
DND OFF	Enter the Do Not Disturb OFF access code.	Yes
Call Forward All ON	Enter the Call Forward All ON access code. As a Comverse feature, the code supports value substitution. For example, if an ON code is configured as *71%N#, %N will be replaced by another value before it is used as the INVITE target.	Yes
Call Forward All OFF	Enter the Call Forward All OFF access code. As a Comverse feature, the code supports value substitution.	Yes
Call Forward No Answer ON	Enter the Call Forward No Answer ON access code.	Yes
Call Forward No Answer OFF	Enter the Call Forward No Answer OFF access code.	Yes
Call Forward Busy ON	Enter the Call Forward Busy ON access code.	Yes
Call Forward Busy OFF	Enter the Call Forward Busy OFF access code.	Yes
Anonymous Call Reject ON	Enter the Anonymous Call Reject ON access code.	No
Anonymous Call Reject OFF	Enter the Anonymous Call Reject OFF access code.	No
Anonymous Call ON	Enter the Anonymous Call ON access code.	No
Anonymous Call OFF	Enter the Anonymous Call OFF access code.	No
Call Waiting ON	Enter the Call Waiting ON access code.	No
Call Waiting OFF	Enter the Call Waiting OFF access code.	No
Group Call Pickup	Enter the Group Call Pickup code. Dialing the code enables the user to answer a call ringing at another VSP861 that is part of the same group.	Yes
Direct Call Pickup	Enter the Direct Call Pickup code. Dialing the code enables the user to answer a call ringing at another VSP861.	Yes

Setting	Description	Assignable to PFK?
Hunt Group Sign ON	Enter the Comverse Hunt Group ON code. Supports value substitution.	Yes
Hunt Group Sign OFF	Enter the Comverse Hunt Group OFF code. Supports value substitution.	Yes
Secretarial Filtering ON	Enter the Comverse Secretarial Filtering ON code. Supports value substitution.	Yes
Secretarial Filtering OFF	Enter the Comverse Secretarial Filtering OFF code. Supports value substitution.	Yes

Busy Lamp Field

Setting	Description
List URI	Enter the BLF list URI, as supplied by or set up with your service provider. For example, blf-list1@sipservice.com. This list contains a list of extensions that are eligible for BLF monitoring. You can assign keys for BLF monitoring on the Programmable Keys page. See *"Programmable Feature Keys" on page 72*.
Remote Pickup Code	Enter the remote pickup code for the BLF list, as supplied by your service provider.
BLF subscription expiration	Enter the BLF subscription expiry time (in seconds) for account x.

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 VSP861 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 VSP861 receives unsolicited MWI notifications.
Enable Stutter Dial Tone	Enables or disables the stutter dial tone for that account (indicating message(s) waiting) when the phone goes off hook.

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 VSP861 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 STUN Keep-Alive	Enables or disables STUN keep-alives. Keep-alive packets are used to maintain connections established through NAT.
Keep-alive interval (secs)	Enter the interval (in seconds) for sending 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.

Jitter Buffer

Setting	Description
Fixed	Enable fixed jitter buffer mode.
Fixed Delay (ms)	If Fixed is selected, enter the fixed jitter delay.
Adaptive	Enable adaptive jitter buffer mode.
Normal Delay (ms)	If Adaptive is selected, enter the normal or "target" delay.
Minimum Delay (ms)	Enter the minimum delay.
Maximum Delay (ms)	Enter the maximum delay. This time, in milliseconds, must be at least twice the minimum delay.

Keep Alive

Setting	Description
Enable Keep Alive	Enable SIP keep alive in service of NAT traversal and as a heartbeat mechanism to audit the SIP server health status. Once enabled, OPTIONS traffic should be sent whenever the account is registered. OPTIONS traffic will occur periodically according to the keep-alive interval.
Keep Alive Interval (secs)	Set the interval at which the OPTIONS for the keep-alive mechanism are sent.
Ignore Keep Alive Failure	Enable the phone to ignore keep-alive failure, if the failure can trigger account re-registration and re-subscription (and active calls are dropped).

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 188*.

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."

Setting	Description
Ringer Tone	Sets the ringer tone for incoming calls on the account.

Do Not Disturb

Setting	Description
Enable DND	Turns Do Not Disturb on or off.
Incoming calls	When set to Show, the phone displays incoming call information while Do Not Disturb is on. When set to Reject, the phone rejects incoming calls without alerting the user.

Auto Answer

Setting	Description
Enable Auto Answer	Enables or disables unconditional Auto Answer. Auto Answer allows a deskset or conference phone to automatically answer incoming calls to that account without user intervention. An auto answer tone will sound.
Auto Answer Delay	Sets the delay before the phone auto answers a call. Before the phone auto answers, the incoming call behaves identical to a normal call. Unless the user responds to the call (with reject, forward, answer, etc.), the phone answers the call after the delay expires. If Auto Answer Delay is set to zero, the incoming call is answered right away without triggering a ringer tone or ringer splash. However, the auto answer tone is still audible.
Enable Mute on Answer	Enables or disables muting the mic upon auto answering. Enabling muting is useful if the auto answered call is for the purpose of a one-way announcement. The user can unmute the call any time after being auto answered.
Ringer Tone	Sets the ringer tone for incoming calls on the account.

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.

Call Completion

When the user calls a busy number, the Call Completion feature enables the phone to redial the busy number automatically. You can configure the redialing to take place after a set interval and for a set number of times.

Call completion settings must be configured for each account.

Setting	Description
Enable Call Completion	Enable or disable the call completion feature. Calls to busy numbers will prompt a "Retry later?" message on the phone screen.
Enable Call Completion Alert	Enables or disables an audible alert (similar to a hold reminder alert tone) if the user is on another call when the auto redial interval expires.
Auto Redial Interval (secs)	Sets the countdown timer until the user is prompted for the next dialing attempt.
Auto Redial Repeat	Sets how many auto redial attempts are made.

Custom Ringer

Setting	Description
Custom Ringer File	Upload a custom ringer audio file. This ringer replaces the factory default ringer 10. The maximum file size is 300 k. The following WAV format is accepted: ■ Audio sample rate: 16 kHz ■ Audio sample size: 16 bit ■ Channels: 1 (mono) ■ Audio format: PCM, Signed 16bit, Little Endian

User Preferences

On the User Preferences page, you can configure some basic settings for the phone and set hold reminder and call waiting settings. The User Preferences page is also available to phone users when they log on to the WebUI.

The user preference settings are also available as parameters in the configuration file. See *"user_pref Module: User Preference Settings" on page 184*.

General User Settings

Click the link for each setting to see the matching configuration file parameter in *"Configuration File Parameter Guide" on page 140*. Default values and ranges are listed there.

Setting	Description
WebUI Language	Sets the language that appears on the WebUI.
Phone Language	Sets the language that appears on the phone. Other languages may be added in a future release.
Backlight Timer (secs)	Sets how long (in seconds) the screen backlight stays on after the last button press.
Ringer Volume	Sets the ringer volume for incoming calls. You can also use the VOLUME ▼ or ▲ keys on the VSP861.

Setting	Description
Default Audio Mode	Sets how calls are answered when users press a line key or **Accept**.
Timeout to Idle Without Digit	Sets the timeout (in seconds) after the phone goes off hook and no digits are entered. After the timeout, the phone returns to idle mode.
Enable Key Beep	Enables or disables key-press beeps.

Call Hold Reminder

Setting	Description
Enable Call Hold Reminder Tone	Enables or disables the call hold reminder tone. Select to enable.
Tone Interval (secs)	Sets the interval for the call hold reminder tone, in seconds.

Call Waiting

Setting	Description
Call Waiting Off	When selected, disables incoming call notifications when the user is already on a call. Incoming calls are rejected. Incoming callers hear a busy signal. When Call Waiting Off is selected, and Call Forward Busy is enabled, incoming calls are handled according to the Call Foward Busy setting.
Call Waiting On	When selected, enables incoming call notifications when the user is already on a call.
Enable Call Waiting Tone	Enables or disables the call waiting tone. Select to enable.
Tone Interval (secs)	Sets the interval for the call waiting tone, in seconds.

Call Transfer

Setting	Description

Quick Transfer via Programmable Keys	Sets transfer options for Quick Dial and BLF Programmable keys during an active call. When a quick dial key or BLF key is pressed during an active call, the key will:
	
	■ Start a new call
	
	■ Perform a blind transfer of the active call to the extension associated with the quick dial or BLF key. This enables one-button operation for Call Park, Park Retrieval, and Park Orbit monitoring.
	
	■ Perform an attended transfer of the active call to the extension associated with the quick dial or BLF key.
	
	The above operations are server dependent. The server has to support all of the following with Call Park to make one-button operation possible:
	
	■ Monitoring a park orbit as an extension via BLF subscription (rfc4235)
	
	■ Remote BLF pickup via one of the two pickup options:
	
	   ● New call via SIP INVITE
	
	   ● Dialog based via SIP INVITE with REPLACE
	
	■ Parking an active call via blind transfer to a park orbit.

Programmable Feature Keys

The Programmable Keys pages allow you to program the Feature Keys Page on the deskset.
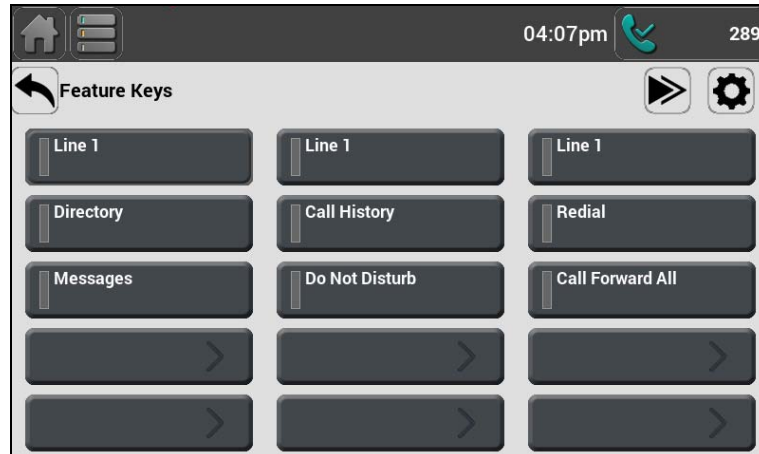
You can assign up to 30 functions to the keys listed on the Feature Keys page.

Keys can have identical functions, depending on the "Type" of key. For example, you can assign several **Line** keys to Account 1 to enable users to manage multiple calls on Account 1. You can also assign multiple **Quick Dial** keys.

The programmable key settings are also available as parameters in the configuration file. See *"pfk Module: Programmable Feature Key Settings" on page 192*.

For the programmable key default settings, see *"Programmable Feature Keys" on page 15*.

Click the link for each setting to see the matching configuration file parameter in *"Configuration File Parameter Guide" on page 140*. Default values and ranges are listed there.

SYSTEM

| STATUS | SYSTEM | NETWORK | CONTACTS | SERVICING |

SIP Account Management
- Account 1
- Account 2
- Account 3
- Account 4
- Account 5
- Account 6
- Account 7
- Account 8

Call Settings
- Account 1
- Account 2
- Account 3
- Account 4
- Account 5
- Account 6
- Account 7
- Account 8

User Preferences

Programmable Keys
- Feature Keys

Speed Dial

Ringer

Paging Zones

Server Application

Hotline Settings

Local Call Recording

Programmable Keys

Key	Type	Label	Value	Account
Key 1	Line			Account 1
Key 2	Line			Account 1
Key 3	Line			Account 2
Key 4	Directory			Account 1
Key 5	Call History			Account 1
Key 6	Redial			Account 1
Key 7	Messages			Account 1
Key 8	Do Not Disturb			Account 1
Key 9	Call Forward All			Account 1
Key 10	N/A			Account 1
Key 11	N/A			Account 2
Key 12	N/A			Account 1
Key 13	N/A			Account 1
Key 14	N/A			Account 1
Key 15	N/A			Account 1
Key 16	N/A			Account 1
Key 17	N/A			Account 1
Key 18	N/A			Account 1
Key 19	N/A			Account 1
Key 20	N/A			Account 1
Key 21	N/A			Account 1

Programmable Key Type	Description
Line	Configures the key for accessing an account. Users can make or answer calls by pressing these keys. The key LED will change according to call activity. After selecting Account in the Type column, select the account number in the Account column.
Directory	Configures the key to access the Directory menu. Users can then press the key to view the Directory menu.
Call History	Configures the key to access the Call History list. Users can then press the key to view the Call History list.
Redial	Configures the key to access the Redial list. Users can then press the key to view the Redial list.
Messages	Configures the key to access the Message menu. Users can then press the key to view the Message menu.
Do Not Disturb	Configures the key to turn Do Not Disturb on or off for a selected account. The key is lit orange when DND is on. If DND is on and a Do Not Disturb All key is also available, the DND All key flashes to indicate that not all accounts have DND set.

Programmable Key Type	Description
Do Not Disturb All	Configures the key to turn Do Not Disturb on or off for all accounts. The key is lit orange when DND All is on (as are any other DND keys). If one or more accounts also has a dedicated DND key, turning DND off for a particular account will cause the DND All key to flash, indicating that not all accounts have DND set.
Call Forward All	Configures the key to turn Call Forward All on or off. In the Account column, select the account for which Call Forward All will apply. Before assigning the key, ensure that you configure Call Forward settings on the Call Settings page.
Call Forward No Answer	Configures the key to turn Call Forward No Answer on or off. In the Account column, select the account for which Call Forward No Answer will apply. Before assigning the key, ensure that you configure Call Forward settings on the Call Settings page.
Call Forward Busy	Configures the key to turn Call Forward Busy on or off. In the Account column, select the account for which Call Forward Busy will apply. Before assigning the key, ensure that you configure Call Forward settings on the Call Settings page.
Quick Dial	Configures the key to dial a number on the selected line. After selecting Quick Dial, enter the number to be dialed in the Value column. In the Account column, select the account on which the number will be dialed out.
BLF (Busy Lamp Field)	Configures the key to monitor another extension. In the Value column, enter the URI of the extension you want to monitor with this key. For example, 2325552001@sipservice.com. For configuring BLF interoperability when using certain service platforms, see `sip_account.x.blf_variant`.
XML App	Configures the key to open the XML browser. Pressing the key initiates an HTTP(s) GET request to the server. Enter the URI of the XML application to be executed.
Page	Configures the key to call one or a group of phones. Pressing the key dials the Paging feature access code. You must enter the feature access code for Paging on the SIP Account Management page. For some service providers, you must also enter a page extension value in the Value column. This value will be dialed along with the Paging feature access code. You can configure pages to be automatically answered. See "Page Auto Answer" under *"SIP Account Management" on page 51*.

Programmable Key Type	Description
Multicast Page	Configures the key to make outgoing multicast pages. In the Value column, enter a valid Paging Zone ID (ranging from 1 to 10). Multicast paging differs from standard paging in that it is handled locally by the VSP861 and does not require a subscription through the hosted server. To use multicast paging, you must first set up paging zones on the WebUI. See *"Paging Zones" on page 79*. See also `pfk.x.multicast_zone` in the configuration file.
Park Call	Enables the user to park a call. Pressing the key dials the Call Park feature access code (FAC). You must enter the feature access code for Call Park on the SIP Account Management page. For some service providers, you must also enter a park extension in the Value column. This value will be dialed along with the Call Park FAC. See also `sip_account.x.park_variant.`
Retrieve Parked Call	Enables the user to retrieve a parked call. Pressing the key dials the Parked Call Retrieval feature access code (FAC) configured on the SIP Account Management page. For some service providers, you must also enter a park retrieval extension in the Value column. This value will be dialed along with the Parked Call Retrieval FAC.
In Call DTMF	Configures the key to dial a string of numbers while the end user is on a call. For example, pressing the key might dial a conference access code. After selecting In Call DTMF, enter the number to be dialed in the Value column. See also `pfk.x.incall_dtmf` in the configuration file.
Call Return	Configures the key to dial the number of the last missed call.
Group Call Pickup	Enables the user to answer a call ringing at another extension. The call can be ringing at any extension in the phone's call pickup group. Pressing the key dials the Group Call Pickup feature access code (FAC) configured on the SIP Account Management page.
Direct Call Pickup	Enables the user to answer a call ringing at a specific VSP861 or compatible SIP telephone. Pressing the key dials the Direct Call Pickup feature access code (FAC) configured on the SIP Account Management page. Depending on the server requirements, the user may then need to enter the number of the ringing extension.

Programmable Key Type	Description
Prefix Dialing	Configures the key for prefix dialing. Pressing a PFK assigned to Prefix Dialing will automatically go off-hook into Dial mode using the account configured for the PFK. The digits entered under **Value** are concatenated to any number that the user enters. The outgoing call will include the [Prefix] + [Dialing string]. The Prefix digits are hidden from the user. The prefix digits are visible during Dialing and Call Active states. Note that **%N** can be used for substitution of user-entered digits. For example, ***71%N#** will use [*71] + [user-entered digits] + [#] as the outgoing dialing string. The dial plan is enabled after the user enters one or more digits. Both prefix digits (hidden) and user-entered digits (visible) are used for dial plan matching. The timeout-to-dial element in the dial plan is suspended if the user navigates away from the dialing screen.
Flash	Configures the key as a Flash key. With one call active, pressing Flash puts the active call on hold and displays a new call screen with live dial. With two calls active, pressing Flash: ■ puts the active call on hold and retrieves a held call, or ■ answers an incoming call.
Call Handling Profile	Configures the key for Comverse call handling profile. Enter the string of the call handling profile that the PFK LED will indicate.
Hunt Group	Configures the key to turn Comverse hunt group on or off. Enter the hunt group extension number assigned for this key.
Secretarial Filtering	Configures the key to turn Comverse secretarial filtering on or off. Enter the manager's extension number assigned for this key.
Phone Lock	Configures the key to enable or disable the phone lock. For more information, see *"Using the Phone Lock menu" on page 41* and *"Security" on page 121*.

Speed Dial Keys

On the Speed Dial page, you can enter up to 10 speed dial numbers. For each speed dial number you enter, you must assign the account on which the number will be dialed out.

To dial a speed dial number, press and hold the dial pad key that matches the speed dial entry number.

> **NOTE** This menu duplicates the speed dial menu on the phone (**Main Menu > Features > Speed dial**). Entries that are entered and saved on the WebUI replace entries that were entered using the phone. Similarly, entries that are configured using the phone menu will update entries on the WebUI.

The speed dial key settings are also available as parameters in the configuration file. See *"speed_dial Module: Speed Dial Settings" on page 196*.

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

SYSTEM	STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING

SIP Account Management
- Account 1
- Account 2
- Account 3
- Account 4
- Account 5
- Account 6
- Account 7
- Account 8

Call Settings
- Account 1
- Account 2
- Account 3
- Account 4
- Account 5
- Account 6
- Account 7
- Account 8

Speed Dial

Key	Name	Value	Account
Key 1			Default
Key 2			Default
Key 3			Default
Key 4			Default
Key 5			Default
Key 6			Default
Key 7			Default
Key 8			Default
Key 9			Default
Key 0			Default

Save

To enter speed dial numbers:

1. In the **Name** column, enter the name associated with this speed-dial entry.

2. In the **Value** column, enter a phone number for the desired key.

3. In the **Account** column, select the account that this speed dial number will use.

4. Click **Save** .

Speed Dial Keys

Click the link for each setting to see the matching configuration file parameter in *"speed_dial Module: Speed Dial Settings" on page 196*.

Setting	Description
Name	The name associated with the speed dial entry.
Value	The phone number that the speed dial key dials when pressed and held.
Account	The SIP account that the phone will use to dial the number.

Ringer Settings

The Ringer Settings enable you to provide a distinctive ringing feature via the custom Alert-Info header associated with an incoming call. This setting overrides the ringer tone you have set for the account. For example, you can set a unique ringer tone to alert the VSP861 user upon receiving any incoming calls tagged as "important" in the Alert-Info header.

The SIP Invite message contains an Alert-Info header that the phone checks in order to determine which ringer tone to play. The Alert-Info header format is as follows:

```
Alert-Info: info=info_text
```

If the header contains the "info" parameter, the phone attempts to match it to the Distinctive Ringing Text. If there is a match, the associated tone will play. If there is no match, the default tone for the account will play.

The matching is done on a "first match" basis. In the case of duplicate text strings, the ringer tone associated with the first matched entry in the Distinctive Ringing Text list will play.

The server-side configuration must be done with your service provider. The SIP Invite text ("Distinctive Ringing Text" on the Ringer WebUI page) must be entered in the format **ringerx**, where x is the ringer number from 1 to 10. For example, to match Ringer 1 enter **ringer1**.

The ringer settings are also available as parameters in the configuration file. See *"ringersetting Module: Distinctive Ringer Settings" on page 199*.

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

Setting	Description
Distinctive Ringing Text	Enter the text that will match the "info" parameter and play the ringer tone. The Distinctive Ringing Text must be in the format **ringerx** where x is the ringer tone 1 to 10.
Tone	Select the desired ringer from the list.

Paging Zones

On the Paging Zones page, you can enter the multicast IP addresses that the phone will monitor. When a page is sent out using this multicast IP address, all phones that are programmed to monitor that IP address will receive the paging RTP stream and play the page on their speakerphone. You can also enable the phone to send out multicast pages using a particular multicast IP address.

You must first set up paging groups (each group consisting of a multicast paging IP address and assigned User IDs) on your SIP PBX. The VSP861 can monitor a maximum of 10 multicast IP addresses.

Setting	Description
Name	Enter the name of the paging zone. Names can be a maximum of 15 characters. The paging zone name is displayed on the LCD during incoming and outgoing multicast pages.
Multicast IP	Enter the paging zone multicast IP address. The IP address range for multicast addresses is 224.0.0.0–239.255.255.255.
Multicast Port	Enter the multicast port used by the multicast IP address. The valid port range is 1 to 65535.
Priority	Select the paging zone priority from 1 to 10. Zones with a priority higher than another zone can interrupt the lower-priority zone's active page. In addition, a call priority setting is available in the configuration file (page_zone.call_priority_threshold). This priority setting also ranges from 1 to 10 (2 is the default). If the paging zone priority is higher or equal to the call priority, then a multicast page can interrupt an active, dialing, or incoming call.
Enable Incoming Page	Select to enable the VSP861 to receive incoming pages for that paging zone. If the "Enable Incoming Page" checkbox is not selected, the phone will not listen for the multicast, but will still be able to broadcast an outgoing page.

Server Application

On the Server Application page, you can enter Action URIs to allow the VSP861 to interact with a server application by using an HTTP GET request. The action URI triggers a GET request when a specified event occurs. Action URIs allow an external application to take control of the display when an event occurs. These pre-defined events are listed under "Action URI" on the Server Application page.

Action URIs are typically used in conjunction with the XML Browser, which can be customized to deliver an appropriate user experience.

The VSP861 supports both push and pull server applications. Note that Action URI events are not "push" events as it is the phone that requests a URI when triggered by certain states. You can enable push server applications under "XML Push Settings".

Action URI Syntax

To access an XML application, the phone performs an HTTP GET on a URL.

An HTTP GET request may contain a variable name and variable value, which are separated by "=". Each variable value starts and ends with "$$" in the query part of the URL.

Action URI variables pass dynamic data to the server. The valid URL format is:
`http://host[:port]/dir/file name?variable name=$$variable value$$`

where:

- host is the hostname or IP address of the server supporting the XML application

- port is the port number the phones are using for the HTTP request

At the time of the HTTP call, the variable value field is populated with the appropriate data. For example, the following URL passes the SIP Account User Identifier to the server:
`http://10.50.10.140/script.pl?name=$$SIPUSERNAME$$`

A GET request then passes along the following information:
`http://10.50.10.140/script.pl?name=42512`

Assuming that the User Identifier is 42512.

Variable names are defined by the particular XML application being called.

Variable values are predefined and depend on the status of the phone. If the variable has no meaning in the current status, then the phone sends an empty string.

The table below lists all possible variable values. Note that variables applicable during an Incoming or Active Call (such as INCOMINGNAME and REMOTENUMBER) are initialized at the beginning and at the end of the call.

Variable value	Description
SIPUSERNAME	SIP Account User Identifier
DISPLAYNAME	SIP Account Display Name

Variable value	Description
LOCALIP	Phone's local IP Address
INCOMINGNAME	Caller ID name of the current Incoming Call
REMOTENUMBER	Remote party phone number (Incoming or Outgoing)
REGISTRATIONSTATE	Registration state available from the Registration event. Values are: ■ REGISTERED ■ DEREGISTERED ■ FAIL
MAC	The phone's MAC Address
MODEL	The phone's model number: VSP861.

Action URI

Setting	Description
End of boot sequence	The End of boot sequence URI is triggered at the end of the phone boot sequence. Using the End of boot sequence URI, it is possible to develop self-provisioning on the phone. For example, an XML application can identify the phone and generate a MAC-specific file on the fly.
Successful Registration	The Successful Registration URI is triggered the first time the phone registers successfully to a SIP Account. If the phone registers to multiple SIP Accounts, then the Successful Registration URI is triggered for each line.

Setting	Description
On Hook	The On Hook URI is triggered when the phone transitions from Active to Idle (or from Paging to Idle). For example, when: ■ The user presses the **End** button ■ The user hangs up the corded handset during a call ■ A transfer is completed and the user returns to idle ■ The far end hangs up ■ The call was not answered ■ The call fails.
Off Hook	The Off Hook URI is triggered when the user goes to Dial mode by: ■ Lifting the corded handset of the cradle ■ Pressing the SPEAKER or HEADSET hard key ■ Pressing a Line PFK ■ Pressing the [New] button during a held call. Note that the Off Hook URI will NOT be triggered when calling a pre-defined number and going immediately to Dialing mode—this event triggers the Outgoing Call URI instead.
Incoming Call	The Incoming Call URI is triggered for each Incoming Ring event or Call Waiting event. Using the Incoming Call URI, it is possible to display extra information on the phone for an Incoming Call. For example, the XML application that is called when there is an Incoming Call can do a database lookup and display information on the caller. Note that this Action URI will not be triggered if DND or Call Forward All is enabled or if Call Waiting is disabled (i.e., the call is rejected).
Outgoing Call	The Outgoing Call URI is triggered each time a SIP INVITE message is sent (Dialing mode). For example, after: ■ Pressing the **Dial** key in Pre-Dial with populated number ■ Using the dial pad to speed dial a call ■ Pressing a Quick Dial PFK ■ Dialing a Directory number by going off-hook.
Timer Based	The Timer Based URI will be triggered when the configured timeout expires. The timer starts at the end of the phone boot sequence.
Timer Based Interval	Enter the interveral before the Timer Based URI is triggered.

Setting	Description
Connected	The Connected URI is triggered each time the phone is in an Active Call or is Paging.
Registration Event	The Registration Event URI is triggered every time there is a registration state change. For example: ■ Registered ■ Deregistered ■ Fail (Registration timed out, refused, or expired) The Registration Event URI is not triggered when the same event is repeated.

XML Push Settings

Setting	Description
Enable HTTP Push	Select to enable HTTP push, which enables the phone to display XML objects that are "pushed" to the phone from the server via http/https POST or SIP NOTIFY.
Enable Push during call	Select to enable the phone to display pushed XML objects during a call. Otherwise, the XML application is displayed after the call is over.

Hotline Settings

Hotline settings enable the VSP861 to dial a pre-configured number after any off-hook action in idle mode—lifting the handset, pressing **SPEAKER**, pressing **HEADSET**, or pressing a PFK Line key. The hotline dialing is subject to a delay. When this delay is configured, it supercedes the inter-digit timeout used for regular calls.

Predial mode and dialing mode are not considered idle mode. Hotline dialing will not trigger if digits have been entered, or when the phone is dialing a number.

Hotline dialing will be cancelled if the user presses any keys, or if there are any incoming calls during the hotline dialing delay period.

The hotline number uses the phone's default dial plan.

Setting	Description
Enable Hotline	Enables the hotline feature.
Account	Sets the account used for dialing the hotline number.
Phone Number	Sets the number to be dialed after the hotline delay.
Delay (secs)	Sets the hotline delay before the number is dialed.

85

Local Call Recording

You can enable or disable local call recording and the call record tone on the Local Call Recording page. You can also delete recordings or export call recordings to the computer.

NOTE	Before enabling call recording on the Local Call Recording page, an SD card must be inserted into the slot on the rear of the deskset.

Setting	Description
Enable Call Recording	Enable call recording for end users.
Enable Call Recording Tone	Enable a call recording tone that plays during the call when recording begins and ends.

Network Pages

You can set up the VSP861 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 VSP861 settings must match the network settings.

The network settings are grouped into Basic and Advanced Settings. IPv4 and IPv6 protocols are supported.

When both IPv4 and IPv6 are enabled and available, the following guidelines apply when determining which stack to use:

- For outgoing traffic, the IP address (or resolved IP) in the server field—either IPv4 or IPv6—will determine which stack to be used.

- In general, most operations can be associated with one of the servers listed on the "Basic Network Settings" page. However, for operations triggered by/dependent upon network status, the phone must determine which server to use. For example, a special case like the "Network down" icon on the Deskset screen can be ambiguous for server association. Because its primary purpose is to aid in troubleshooting SIP registration issues, this case will be associated with the SIP registration server.

- DNS entries with both IPv4 and IPv6 settings can be used to resolve FQDN entries. There are no preferences with the order of the DNS queries.

- Pcap should include traffic for both stacks.

- Dual stack operations should be transparent to PC port traffic.

NOTE
- PnP is not supported on IPv6.
- VPN is not supported in IPv6 or PPPoE.

The network settings are also available as parameters in the configuration file. See *"network Module: Network Settings" on page 158*.

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

Basic Network Settings

> **NOTE** 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 158*. Default values and ranges are listed there.

IPv4

Setting	Description
Disable	Disables all related IPv4 settings.
DHCP	DHCP is selected (enabled) by default, which means the VSP861 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 VSP861, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).

Setting	Description
Static IP	When Static IP is selected, you must enter a static IP address for the VSP861, 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 VSP861.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the address of the default gateway (in this case, your router).
PPPoE	Select to enable PPPoE (Point-to-Point Protocol over Ethernet) mode.
PPPoE Username	Enter your PPPoE account username.
PPPoE password	Enter your PPPoE account password.
Manually Configure DNS	Select to enable manual DNS configuration.
Primary DNS	If DHCP is disabled, enter addresses for the primary and secondary DNS servers.
Secondary DNS	

IPv6

Setting	Description
Disable	Disables all related IPv6 settings.
Auto Configuration	Auto configuration is selected (enabled) by default, which means the VSP861 will get its IP address, Gateway, and DNS Server(s) from the network. When Auto Configuration is disabled, you must enter a static IP address for the VSP861, as well as addresses for the Gateway and DNS Server(s).
Static IP	When Static IP is selected, you must enter a static IP address for the VSP861, as well as an IPv6 address prefix, Gateway, and DNS Server(s).
IP Address	If Auto Configuration is disabled, enter a static IP address for the VSP861.
Prefix (0–128)	Enter the IPv6 address prefix length (0 to 128 bits).
Gateway	Enter the address of the default gateway (in this case, your router).
Manually Configure DNS	Select to enable manual DNS configuration.
Primary DNS	If Auto Configuration is disabled, enter addresses for the primary and secondary DNS servers.
Secondary DNS	

Advanced Network Settings

PC Port

You can set the availability of the deskset PC port for network connectivity. When the port is enabled for connectivity, you can set the port to port mirroring, thereby allowing you to use the port to monitor inbound and outbound network traffic and facilitate troubleshooting.

Setting	Description
Enable PC Port	Enable or disable the PC port to operate in hub/switch mode (depending on the Enable PC Port Mirroring setting).
Enable PC Port Mirroring	When the PC port is enabled, select Enable PC Port Mirroring to set the port to operate in hub mode (network traffic on the WAN port is reflected in the PC port). When Port Mirroring is not selected, the port operates in switch mode.

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 158*. 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.
Enable PC Port VLAN	Enable if the phone is part of a VLAN on your network. Select to enable.
VID	Enter the PC Port 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.

VPN

You can operate the VSP861 SIP deskset over a Virtual Private Network (VPN). VPN enables remote users and remote sites to connect to a main corporate network and SIP server with a high level of performance and security.

Configuring VPN using the WebUI consists of enabling VPN and uploading a VPN configuration file. The VPN configuration file (**openvpn_client.tar**) must contain the following files:

- **client.conf**
- a **keys** folder containing
    - **ca.crt**
    - **client.crt**
    - **client.key**

The filename of the VPN client configuration file and certificates must match the names provided above. For more information about configuring VPN, visit our website at *businessphones.vtech.com* or call **1 (888) 370-2006**.

> **NOTE** Ensure that NTP or manual time is configured correctly so that the VSP861 is using the correct date and time before VPN setup. Mismatched time between sites and servers may invalidate the initial TLS handshake.

Setting	Description
VPN Enable	Enables or disables the phone to connect using the OpenVPN client. If VPN is enabled, but not connected, all SIP traffic will continue to route via the LAN IP. If VPN is enabled and connected, all SIP traffic will route via the VPN tunnel. The exception is the web server, which will still be accessible via the LAN IP.
VPN Config (file upload)	Browse to and upload the VPN configuration file **openvpn_client.tar**.

Contacts Pages

Local Directory

On the Local Directory page, you can manage your local directory entries. You can sort, edit, delete, and add contact information for up to 1000 entries. In order to back up your contacts or import another local directory file, the page also enables you to export and import your phone's local directory.

The Local Directory lists entries across multiple pages. Click [Next] , [Last] , [First] , or a page number to view the desired page of entries.

> **NOTE** You can also use the phone menu to manage local directory entries. For more information, see the VSP861 User Guide.

Table 6 describes the buttons available on the Local Directory page.

Table 6. Local 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 Local Directory Entry** page appears.

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

Create Local 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–	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. The directory can be exported as an .xml or .csv file. After exporting the file, open it in an .xml or .csv editor and add or modify entries.

> **NOTE** When importing a .csv file, you can select whether the first line should be treated as a header and ignored for the import.

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 Parameters" on page 201*.

Directory files in .xml format 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>

Local Directory WebUI field	Directory file XML tag
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 VSP861 rejects calls from numbers that match blacklist entries. You can sort, edit, delete, and add up to 1000 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 across multple pages. Click [Next] , [Last] , [First] , or a page number to view the desired page of entries.

> **NOTE** You can also use the VSP861 menu to manage blacklist entries. For more information, see the VSP861 User Guide.

Table 7 describes the buttons available on the Blacklist page.

Table 7. 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.

Table 7. Blacklist commands

Click	To...
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.
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 1–8	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 VSP861. The blacklist can be exported as an .xml or .csv file. After exporting the file, open it in an .xml or .csv editor and add or modify entries.

> **NOTE** When importing a .csv file, you can select whether the first line should be treated as a header and ignored for the import.

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 **Delete Selected Entries** 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 Parameters" on page 201*.

Blacklist files in .xml format 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 175*.

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 175*. Default values and ranges are listed there.

About LDAP attribute filters

The LDAP filters on this page give you control over how directory entry search results are determined. For example, consider if **gn** is the firstname attribute and **sn** is the lastname attribute in the LDAP search base. The filter <attribute>=% returns records based on the beginning of the user-entered string. If gn=% is used for a firstname filter, entering "da" returns records such as Daisy, Dale, David, etc.

The filter <attribute>=* returns records containing the user-entered string anywhere in that attribute. If gn=* is used for a firstname filter, entering "ar" returns records such as Karen, Arnold, Gary, etc.

The filter (|(gn=%)(sn=%)) returns firstname and lastname records that start with the user-entered string.

LDAP number filters give you the same control over number searches and matches. If for example, you have defined the number attributes **telephoneNumber**, **mobile** and **otherPhone** for Work, Mobile and Other numbers respectively, then the filter (|(telephoneNumber=*)(mobile=*)(otherPhone=*)) will display the correct directory information if the number (from an incoming call, or a dialed number) matches a number in any three of those fields.

The filter telephoneNumber=* will display the correct directory information if the incoming call number matches a number in the "Work" field only.

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.
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 or LDAP field names, 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.

Setting	Description
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.
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.

Broadsoft

The phone supports access to the Broadsoft Phonebook. Users can search for and call contacts that are hosted on the Broadsoft Phonebook. On the Broadsoft Phonebook Settings page, you must enter the path and credentials to enable the phone to access the Broadsoft Phonebook.

Broadsoft Phonebook Settings

Setting	Description
Enable Broadsoft Phonebook	Enables or disables the phone's access to the Broadsoft phonebook.
Display name	Enter the display name for the Broadsoft Phonebook. This name appears on the Directory list on the VSP861 menu.
Server base address	Enter the Broadsoft Phonebook server domain or IP address.
Port	Enter the Broadsoft Phonebook server port.
Authentication name	Enter the user name or authentication name for Broadsoft Phonebook access.
Authentication password	Enter the authentication password for Broadsoft Phonebook access.
Directory type	Select the directory type: Group, Group Common, Enterprise, Enterprise Common, Personal

Remote XML

The VSP861 supports three server-hosted Remote XML directories. A total of 5000 Remote XML directory entries are supported. The 5000 entries can be shared across the three remote XML directories.

When the user selects a remote directory to view, the VSP861 will sync with the directory server. The phone will display **Sync failed.** if any of the following failing conditions is encountered:

- Server not reachable
- Remote XML directory file is not available
- Invalid XML directory file

Remote XML Directory Format

The following shows a sample single-entry file which can be used in a remote XML directory. Note that the default tags are the same as those defined for the Local Directory.

```
<?xml version="1.0" encoding="utf-8"?>

<DIR_ENTRY>

<DIR_ENTRY_NAME_FIRST>John</DIR_ENTRY_NAME_FIRST>

<DIR_ENTRY_NAME_LAST>Smith</DIR_ENTRY_NAME_LAST>

<DIR_ENTRY_NUMBER_OTHER>3333</DIR_ENTRY_NUMBER_OTHER>

<DIR_ENTRY_NUMBER_WORK>1111</DIR_ENTRY_NUMBER_WORK>

<DIR_ENTRY_NUMBER_MOBILE>2222</DIR_ENTRY_NUMBER_MOBILE>

</DIR_ENTRY>
```

Setting	Description
Name	Sets the name of the directory as it will appear on the VSP861 Directory list. The following order applies to the Directory list when multiple server-based directories are enabled: 1. Local 2. Blacklist 3. LDAP 4. Broadsoft 5. Remote XML directory 1 6. Remote XML directory 2 7. Remote XML directory 3 Any Remote XML directories will move up the list if LDAP and/or Broadsoft directories are not enabled.
Remote XML URI	Enter the location of the XML directory file, from which the phone will sync and retrieve directory entries.
Enable Incoming/ Outgoing Call Lookup	Enables/disables the call lookup feature for incoming and outgoing calls.

Call History

The Call History page has no configurable settings. It displays Missed Calls, Received Calls, and Dialed Calls. Users can view their call history and "click to dial" numbers if click to dial is enabled.

Servicing Pages

Reboot

To manually reboot the VSP861 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 170*.

Time and Date Format

Click the link for each setting to see the matching configuration file parameter in *"time_date Module: Time and Date Settings" on page 170*. Default values and ranges are listed there.

Setting	Description
Date Format	Sets the date format.
Time Format	Sets the clock to a 24-hour or 12-hour format.

Network Time Settings

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

Setting	Description
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 [Apply Now] to start the VSP861 using the manual time settings.

Custom Language

On the Export Translation page, you can export WebUI and/or phone language strings. After exporting language strings, you can use the resulting file as the basis for a custom language translation file (.tpk file).

You can import one custom language for use on the device user interface and the WebUI. The custom language adds to the existing languages available with the firmware. Separate translation files are required for the device user interface and the WebUI.

Importing a custom language can only be done using the configuration file. See *"file Module: Imported File Parameters" on page 201*. For details on creating and formatting a translation file, see the Custom Language document at *businessphones.vtech.com*.

The available languages for export are identical to the WebUI and Phone Language lists described in *"User Preferences" on page 69*.

The filenames of the exported language files will be:

- WebUI: <Model Number>-<Display Name>-webui.tpk

- Device MMI: <Model Number>-<Display Name>-phoneui.tpk

Custom Image/Logo

You can upload a custom image or logo to be displayed on the VSP861 idle screen and during bootup. For more information about formatting a custom logo file, see *"Adding a Custom Logo" on page 21*.

On this page, you can also reset the bootup and idle logos to factory defaults. The default logo for bootup and idle mode is the **vtech** logo.

Setting	Description
Bootup Image/Logo	Import a custom image or logo shown during bootup. For logo specifications, see *"Logo specifications" on page 21*.
Wallpaper	Import an image that will appear as the background of the Home screen.

Firmware Upgrade

You can update the VSP861 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 VSP861 firmware.

The firmware upgrade settings are also available as parameters in the configuration file. See *"provisioning Module: Provisioning Settings" on page 163*.

Firmware Server Settings

Click the link for each setting to see the matching configuration file parameter in *"provisioning Module: Provisioning Settings" on page 163*. Default values and ranges are listed there.

Setting	Description
Firmware URL	The URL where the firmware update file resides. This should be a full path, including the filename of the firmware file.
Handset Firmware URL	The URL where the Cordless Handset Accessory 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 Deskset Firmware Now]   or   [Install Handset Firmware Now] .

> **NOTE** You can also configure the VSP861 to check for firmware updates at regular intervals. See *"Provisioning" on page 114*.

Manual Firmware Update and Upload

On the Manual Firmware Update Settings page, you can upgrade the VSP861 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 VSP861 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 deskset. Second, you must install the handset firmware on the handset. The handset downloads the firmware over the air from the deskset.

To install the handset firmware on the deskset:

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.

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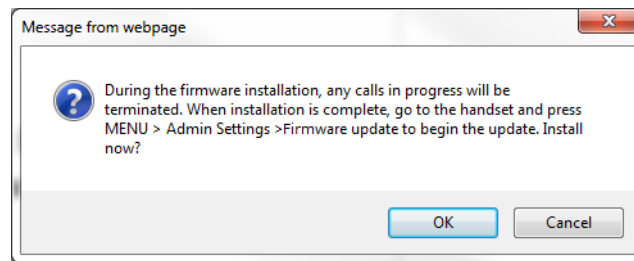
2. To install the handset firmware, click [OK] . The message **Installing handset firmware. Please wait...** appears. To cancel the download, click [Cancel] .

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.

Provisioning

Provisioning refers to the process of acquiring and applying new settings for the VSP861 using configuration files retrieved from a remote computer. After a VSP861 is deployed, subsequent provisioning can update the VSP861 with new settings; for example, if your service provider releases new features. See also *"Provisioning Using Configuration Files" on page 132*.

With automatic provisioning, you enable the VSP861 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 VSP861 settings (configuration and/or firmware) yourself via **Provisioning > Import Configuration** and/or **Firmware Upgrade > Manual Upgrade**. Manual provisioning can only be performed on one VSP861 at a time.

On the Provisioning page, you can enter settings that will enable the VSP861 to receive automatic configuration and firmware updates. The Provisioning page also allows you to manually update VSP861 configuration from a locally stored configuration file using an Import function. You can also export the VSP861 configuration—either to back it up or apply the configuration to another VSP861 in the future—to a file on your computer.

The provisioning process functions according to the Resynchronization settings and Provisioning Server Settings. The VSP861 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 VSP861 updated to the latest firmware release will have the Redirection Server URL available as the default Provisioning Server URL (see *"provisioning.server_address"*).

> **NOTE** 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 VSP861 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 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. The default URL is the VTech redirect server: https://et.vtechphones.com/rg2/
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 VSP861 to search for the provisioning URL via a SUBSCRIBE message to a multicast address (224.0.1.75). The VSP861 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 VSP861 to use DHCP options to locate and retrieve the configuration file. When selected, the VSP861 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.

Setting	Description
User Class Info (DHCP 77)	DHCP Option 77 is available to send vendor-specific information to the DHCP Server.
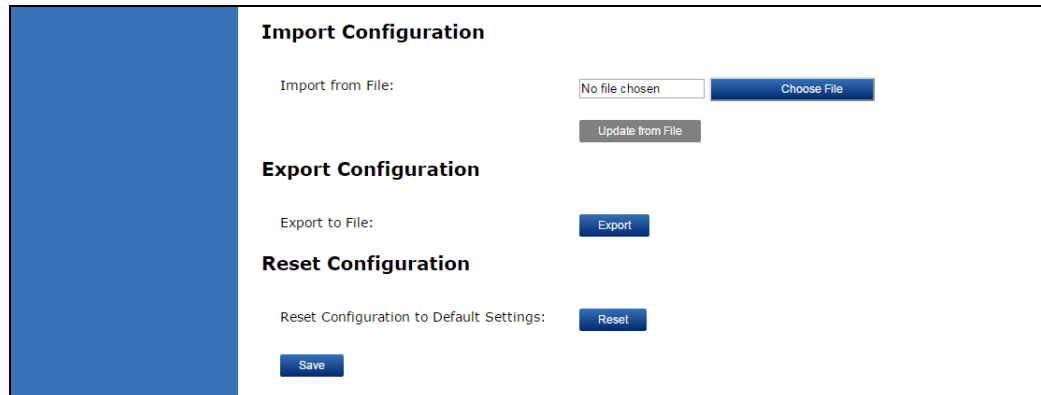
Resynchronization

Setting	Description
Mode	Sets which files for which the VSP861 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 VSP861 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 VSP861 checks for updates.
Start Hour	Select the hour of the day on which the VSP861 checks for updates.
End Hour	Select the hour of the day on which the VSP861 stops checking for updates.

Setting	Description
Use encryption	Enables an AES-encrypted configuration file to be decrypted before being applied to the VSP861. Select if the configuration file has been secured using AES encryption. See *"Securing configuration files with AES encryption" on page 138*.
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 138*.
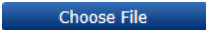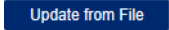
Import Configuration

You can configure the VSP861 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 132*.

To import a configuration file:

1. Click [Choose File] to locate and open the configuration file.

2. Click [Update from File].

The VSP861 will update its configuration.

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

■ The VSP861 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 VSP861 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.

> The exported configuration file will contain null values for the following passwords:
>
> - SIP account authentication password
> - EAPOL password
> - PPPoE password
> - Firmware server password
> - Provisioning server password
> - Encryption passphrase
> - TR-069 password
> - TR-069 connection request password
> - Administrator access password
> - User access password
> - LDAP server password
> - Broadsoft directory server password.
>
> Please ensure that you save the exported configuration file in a secure location. You can also enable passwords to be exported as plain text.
> See *"provisioning.pwd_export_enable" on page 167*.

To export the configuration file:

- Click Export .

The format of the exported file is **<model name>_<mac address>.cfg**. For example, **VSP861_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 VSP861 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, configure the phone lock feature, and enter web server settings.

NOTE By default, after bootup, the VSP861 alerts you if the default passwords (user password and admin password) are still in use.

The security settings are also available as parameters in the configuration file. See *"web Module: Web Settings" on page 181*.

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 216*.

To change the admin password:

1. Enter the old password (for a new VSP861, 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 216*.

To change the User password:

1. Enter the old password (for a new VSP861, 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] .

Phone Lock

The Phone Lock feature restricts certain hard keys and features unless the user enters a PIN code. For more information about the phone lock feature, see *"Using the Phone Lock menu" on page 41*.

Setting	Description
Lock Type	Unrestricted, Emergency Call Only.
Phone Unlock PIN	Enter the PIN that the user enters to unlock the phone.
Auto Lock Timeout (secs)	Enter a timeout period in seconds. When the phone becomes idle after being used in unlocked mode, the phone automatically locks after the timeout.
Restricted Account	Select the account to be used when Phone Lock is active.

PIN Masking

The PIN masking feature allows users to hide PIN numbers during call operation. The different types of PIN masking are:

- Hide DTMF digits—when Hide DTMF is enabled, PIN numbers entered during an Active Call are automatically masked.

- Password Dial—when Password Dial is enabled, PIN numbers entered as part of the dial string are hidden according to the Password Dial Prefix and Password Dial Length settings described below.

PIN numbers in a dial string are masked in Pre-Dial and Dial modes (including variants of these modes, such as Transfer Setup, Conference Setup, and Incoming Call Forward Setup).

> **NOTE** Masked PIN numbers are not saved in Redial entries. The masked numbers are stripped out of the dial string before being saved in the Call History.

Pin Masking

☐ Enable Hidden DTMF digits
☐ Enable Delay for Hidden DTMF digits
☐ Enable Password Dial
☐ Enable Delay for Password Dial
Password Dial Prefix: [   ]
Password Dial Length: [1   ▼]

Setting	Description
Enable Hidden DTMF digits	Enable to mask all DTMF digits entered during an Active Call. Note that unlike Password Dial, there is no prefix parameter and no length parameter, so any DTMF string of any length is masked.
Enable Delay for Hidden DTMF digits	Enable to add a one-second delay before DTMF digits are masked. By default, the digits are masked immediately.
Enable Password Dial	Enable to hide PIN numbers entered as part of the dial string.
Enable Delay for Password Dial	Enable to add a one-second delay before PIN numbers are masked. By default, the PIN number is masked immediately.
Password Dial Prefix	Enter the prefix that serves as an indicator that the next x digits are masked (x being equal to the Password Dial Length). Only the first matched Prefix initiates PIN masking. If additional instances of the Password Dial Prefix appear elsewhere within the dial string, they are ignored.
Password Dial Length	Enter the PIN number length. All digits within this length are masked. Any digits beyond this length are not masked. For example, if the Password Prefix is **99** and the Password Dial Length is **3**, then **9912345** will be rendered as **99***45**.

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 VSP861.

Trusted Servers

The Trusted Servers setting provides a means of blocking unauthorized SIP traffic. When enabled, each account's Registration server, SIP server, Outbound Proxy server and Backup Outbound Proxy server will be used as sources for trusted SIP traffic. All unsolicited SIP traffic (for example, INVITE, NOTIFY, unsolicited MWI, OPTIONS) will be blocked unless it is from one of the trusted servers with the enabled accounts.

If additional trusted sources are required beyond what has been specified with the enabled accounts (for example, if IP dialing or other types of server traffic need to be secured), use the Trusted IP settings on the Security page.

Trusted Servers

☐ Accept SIP account servers only

Setting	Description
Accept SIP account servers only	Enable or disable using the account servers as sources for trusted SIP traffic.

Trusted IP

In addition to the Trusted Servers setting, incoming IP traffic can be filtered using an "Allowed IP" list of IP addresses. When this means is enabled, all unsolicited IP traffic will be blocked unless it is from one of the trusted IP addresses on the "Allowed IP" list.

Yu can enter the "Allowed IP" list in the 10 fields on the "Trusted IP" section. Entries on the "Allowed IP" list must be specified as IP addresses (IPv4 or IPv6).

Three formats are supported for entries on the "Allowed IP" list:

1. IP range specified using CIDR notation (defined in rfc4632). IPv4 or IPv6 address followed by a prefix; for example, 192.168.0.1/24.

2. IP range specified with a pair of starting and ending IPv4 or IPv6 addresses, separated by '-' (for example, 192.168.0.1-192.168.5.6).

   - No space before or after '-'

   - Both starting IP & ending IP have to be with the same IP version

   - Starting IP has to be smaller than the ending IP; otherwise, all traffic will be dropped.

3. Single IP address in IPv4 or IPv6.

> **NOTE** To ensure WebUI access after configuring Trusted IP, you must include the IP of the Web Browser on the "Allowed IP" list.

Trusted IP

☐ Accept only allowed IP for incoming requests

Allowed IP 1:	
Allowed IP 2:	
Allowed IP 3:	
Allowed IP 4:	
Allowed IP 5:	
Allowed IP 6:	
Allowed IP 7:	
Allowed IP 8:	
Allowed IP 9:	
Allowed IP 10:	

[Save]

Setting	Description
Accept only allowed IP for incoming requests	Enable or disable using the "Allowed IP" list to filter all IP traffic.
Allowed IP 1–10	Enter IP addresses or address ranges to be used as sources of authorized IP traffic.

Certificates

You can add two types of certificates using the WebUI or the provisioning file (see *"file Module: Imported File Parameters" on page 201*). The two types of certificates are:

■ Device—A single Device Certificate can be uploaded so that other parties can authenticate the phone in the following cases:

- When the phone acts as a web server for the user to manage configurations.

- When the phone acts as a client for applications where HTTP is supported.

■ Trusted—Trusted Certificates are for server authentication with secured HTTP transaction in the following applications: SIP signaling, Provisioning, Firmware, LDAP directory service, and Broadsoft directory service. Up to 20 trusted certificates can be installed.

Device Certificate

To upload a device certificate:

1. On the Device Certificate page, click **Choose File** .

2. Locate the certificate file and click **Open**.

3. On the Device Certificate page, click **Import** .

Trusted Certificate

On the **Trusted Certificate** page, you can:

- import up to 20 trusted certificates.

- delete individual (or all) certificates.

- protect certificates by selecting them in the **Protected** column, and then clicking [Protect Selected Entries] . Protected certificates cannot be selected for deletion and are not removed during a reset to factory defaults.

Select **Only accept trusted certificates** to enable server authentication. Deselecting this option disables server authentication.

TR-069 Settings

The Broadband Forum's Technical Report 069 (TR-069) defines a protocol for remote management and secure auto-configuration of compatible devices. On the TR069 page, you can enable TR-069 and configure access to an auto-configuration server (ACS).

Setting	Description
Enable TR069	Enable/Disable TR-069 subsystem.
ACS Username	User name used for ACS authentication.
ACS Password	Password used for ACS authentication.
ACS URL	URL used to contact the ACS (for example, http://my.acs:9675/path/to/somewhere/).
Enable Period Inform	Enable/Disable periodic inform method calls.
Periodic Inform Interval (seconds)	Periodic inform method calls interval.
Connection Request Username	If the ACS wants to communicate with the device, it must offer the matching Connection Request user name. When the device sends the report to ACS for the first time, it contains information for this.
Connection Request Password	If the ACS wants to communicate with the device, it must offer the matching Connection Request password. When the device sends the report to ACS for the first time, it contains information for this.

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: System Log Settings" on page 174*.

Syslog Settings

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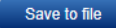
Setting	Description
Log Level	Sets the log level. The higher the level, the larger the debug output. ■ 5—ALL ■ 4—DEBUG ■ 3—INFO ■ 2—WARNING ■ 1—ERROR ■ 0—CRITICAL

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.

C H A P T E R   4

PROVISIONING USING CONFIGURATION FILES

Provisioning using configuration files is the quickest way to configure multiple VSP861 desksets. You can place configuration files on a provisioning server, where the VSP861 desksets retrieve the files and update their configuration automatically.

Configuration files have the extension **.cfg** and contain settings that will apply to VSP861 desksets. 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 VSP861 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 VSP861 configuration file modules and their associated parameters, see *"Configuration File Parameter Guide" on page 140*.

Using the WebUI, you can also import a configuration file and apply the configuration file settings to the VSP861. For more information, see *"Import Configuration" on page 118*.

This chapter covers:

- *"The Provisioning Process" on page 133*

- *"Configuration File Types" on page 135*

- *"Data Files" on page 136*

- *"Configuration File Tips and Security" on page 137*.

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 114* and *"Resynchronization: configuration file checking" on page 134*. The VSP861 maintains a list of the last loaded provisioning files. The VSP861 compares its current configuration against the files it finds on the provisioning server. **Checking for update…** appears on the VSP861 screen.

   If provisioning has been triggered by the resync timer expiring or by remote check-sync, the VSP861 checks for updated files after one minute of inactivity.

2. Download the configuration files.

   If any file on the provisioning server has changed, the VSP861 treats it as a new file and downloads it. **Configuring Deskset…** appears on the VSP861 screen.

   If the provisioning URL specifies a path only with no filename (if the URL ends with "/"), then by default the VSP861 looks for and retrieves the following two files by appending the two default filenames to the URL:

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

   The <model> variable is the VTech product model: VSP861, for example.

   If the provisioning URL contains a query element (?), or a filename ending in ".cfg" is specified at the end of the provided URL path, then the VSP861 retrieves only the configuration file specified.

3. The VSP861 restarts after one minute of inactivity. **Please wait while the phone reboots** appears on the VSP861 screen. For more information, see *"VSP861 restart" on page 134*.

During provisioning, the VSP861 reads the configuration file and validates each module and setting. The VSP861 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 140* 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 VSP861 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 VSP861 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 VSP861 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).

VSP861 restart

If the VSP861 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 VSP861 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 VSP861 will download the file(s) when there is no call activity.

When you update the VSP861 by importing a configuration file using the WebUI, the device restarts immediately after applying the new settings, regardless of whether the VSP861 is idle.

Configuration File Types

The VSP861 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 VSP861 in the system.

The MAC-specific configuration file is a file that only a single VSP861 can retrieve. The MAC-specific configuration file name contains a VSP861 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, **VSP861**. For more information about the MAC-specific configuration file, see *"Guidelines for the MAC-Specific configuration file" on page 137*.

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 VSP861 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 VSP861 desksets in the general file, and then overwrite that setting for just a few VSP861 desksets 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, LDAP, Broadsoft) in pem format

- Logos (a bootup logo and an idle screen logo) in .bmp 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 VSP861 deskset may require.

None of the data files are exported when you export a configuration file from the VSP861. 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 VSP861 import the new file. For a complete list of data file parameters, see *"file Module: Imported File Parameters" on page 201*.

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) VSP861 desksets. 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 VSP861.

Clearing parameters with %NULL in configuration file

For configuration file parameters that can have a text string value, you can clear the value of the parameter by applying the value %NULL in the configuration file.

For example: `sip_account.1.display_name = %NULL`

However, the following parameters are exceptions. Applying the value %NULL to these parameters will reset them to their default value.

- **file.bootup_logo** - applying %NULL restores the default value (VTech logo)

- **file.idle_logo** - applying %NULL restores the default value (VTech logo)

- **file.custom_ringer** - applying %NULL restores the default value

Guidelines for the MAC-Specific configuration file

The VSP861 downloads the MAC-specific configuration file after the general configuration file. You must create a MAC-specific configuration file for each VSP861 in your system. The file name must contain the VSP861 MAC address, which is printed on a label on the back of the device, or available on the **MENU > Status > Product Info** screen. For example, a VTech VSP861 deskset with the MAC address of 00:11:A0:10:6F:2D would download the **VSP861_0011A0106F2D.cfg** file.

> **i NOTE** 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 VSP861 deskset. 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 VSP861 firmware decrypts files using the AES 256 algorithm. After encrypting a file and placing it on your provisioning server, you can enable the VSP861 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 VSP861. 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.
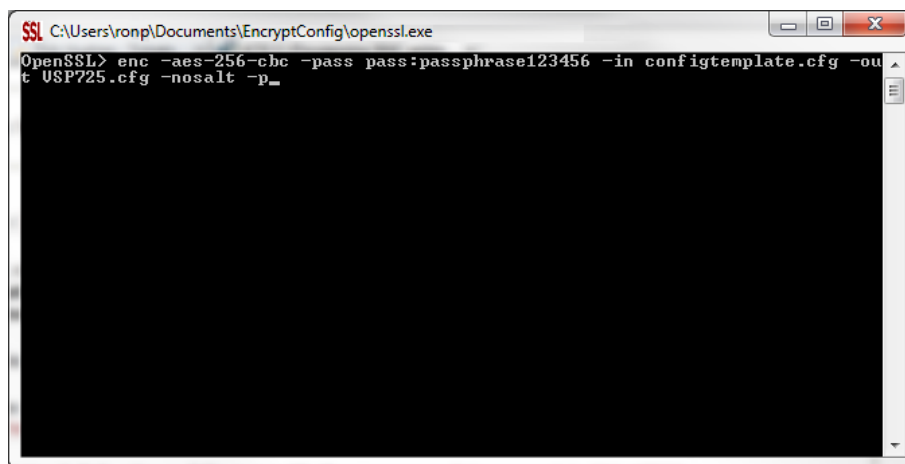
Figure 2. OpenSSL command line

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**.

Resynchronization

Mode:	Both
Bootup Check:	Off
Interval:	0
☑ Use encryption for configuration file	
Passphrase	

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.

C H A P T E R 5

CONFIGURATION FILE PARAMETER GUIDE

This chapter lists the available options for all the settings within the VSP861 configuration file. Most settings in the configuration file have an equivalent in the WebUI (see the settings tables in *"Using the WebUI" on page 45*). 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 VSP861 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" on page 141*

- *"hs_settings Module: Handset Settings" on page 157*

- *"network Module: Network Settings" on page 158*

- *"provisioning Module: Provisioning Settings" on page 163*

- *"security Module: Security Settings" on page 168*

- *"time_date Module: Time and Date Settings" on page 170*

- *"log Module: System Log Settings" on page 174*

- *"remoteDir Module: Remote Directory Settings" on page 175*

- *"web Module: Web Settings" on page 181*

- *"trusted_ip Module: Trusted IP Settings" on page 182*

- *"trusted_servers Module: Trusted Server Settings" on page 183*

- *"user_pref Module: User Preference Settings" on page 184*

sip_account Module: SIP Account Settings

The SIP Account settings enable you to set up individual accounts for each user. 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 for the VSP861.

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 for the VSP861.

All these settings are exported when you manually export the configuration from the VSP861.

General configuration file settings

Setting:	`sip_account.x.dial_plan`
Description:	Sets the dial plan for account x. See *"Dial Plan" on page 54*.
Values:	Text string **Default:** x+P

Setting:	`sip_account.x.call_restrict_dial_plan`
Description:	Sets the call restriction dial plan, which prevents users from completing calls to certain numbers for this account.
Values:	Text string **Default:** blank

Setting:	`sip_account.x.emergency_dial_plan`
Description:	Sets the emergency dial plan.
Values:	Text string **Default:** blank

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 VSP861 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– **Default:**

Setting:	`sip_account.x.auto_answer_enable`
Description:	Enables or disables automatic answering of pages for account x.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`sip_account.x.auto_answer_during_active_call`		
Description:	Enables or disables automatic answering of pages for account x when account x has an active call.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`sip_account.x.barge_in_enable`		
Description:	If the shared line type is enabled for account x, enables or disables "barge in" capability for VSP861 desksets with shared accounts.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

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

Setting:	`sip_account.x.unregister_after_reboot_enable`		
Description:	Enables or disables the VSP861 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:	IPv4, IPv6 or FQDN	**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:	IPv4, IPv6 or FQDN	**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:	IPv4, IPv6 or FQDN	**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:	IPv4, IPv6 or FQDN	**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, g723_1, ilbc	**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, g723_1, ilbc	**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, g723_1, ilbc	**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, g723_1, ilbc	**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, g723_1, ilbc	**Default:**	ilbc

Setting:	`sip_account.x.codec_priority.6`		
Description:	Sets the sixth highest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, g723_1, ilbc	**Default:**	g723_1

Setting:	`sip_account.x.codec_priority.7`		
Description:	Sets the lowest-priority codec for account x.		
Values:	none, g711u, g711a, g729, g726, g722, g723_1, ilbc	**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.729 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 Signaling Quality of Service Layer 3 - DSCP for account x.		
Values:	0–63	**Default:**	26

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

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

Setting:	`sip_account.x.blf_variant`
Description:	Sets the BLF operation for account x. This parameter is not available on the WebUI.
	"default" is for Broadsoft or Asterisk depending on the presence of `sip_account.x.blf_list_uri`. "avaya" is designed as an Avaya variant. "extended_blf" is proprietary. "metaswitch" is designated for Metaswitch. "freeswitch" is designated for Freeswitch.

Values:	default, avaya, extended_blf, metaswitch, freeswitch	**Default:**	default

Setting:	`sip_account.x.blf_subscription_expires`
Description:	Sets the BLF subscription expiry time (in seconds) for account x.

Values:	15–65535	**Default:**	3600

Setting:	`sip_account.x.blf_remote_pickup_code`
Description:	Sets the Busy Lamp Field (BLF) remote pickup 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:	15–65535	**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.stutter_dial_tone_enable`
Description:	Enables or disables MWI stutter dial tone for account x.
Values:	0 (disabled), 1 (enabled) **Default:** 1

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:	IPv4, IPv6 or FQDN **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_stun_keep_alive_enable`
Description:	Enables or disables STUN 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_stun_keep_alive_interval`
Description:	Sets the interval (in seconds) for sending keep-alives.
Values:	0–65535 **Default:** 30

Setting:	`sip_account.x.keep_alive_enable`
Description:	Enable SIP keep alive in service of NAT traversal and as a heartbeat mechanism to audit the SIP server health status.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`sip_account.x.keep_alive_interval`		
Description:	Sets the interval (in seconds) for sending keep-alives.		
Values:	1–3600	**Default:**	15

Setting:	`sip_account.x.keep_alive_ignore_failure`		
Description:	Enable the phone to ignore keep-alive failure, if the failure can trigger account re-registration and re-subscription (and active calls are dropped).		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

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.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:	90–65535	**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.park_variant`		
Description:	Selects how the VSP861 handles call parking, depending on the service provider. When the default "broadsoft" variant is selected, calls are parked via a PFK and a feature access code. The target number for the "park" request is formed by concatenating "Call Park FAC" of the call-to-be-parked account and the value entered for the Park PFK. When the "asterisk" variant is selected, calls are parked through a blind transfer to a parking lot extension.The target parking lot extension will be taken from the following order of priority (if both values exist): ■ Park PFK Value ■ Call Park FAC Value		
Values:	broadsoft, asterisk	**Default:**	broadsoft

Setting:	`sip_account.x.server_side_ctrl_variant`		
Description:	Set the server type that will control feature sync and FAC operation.		
Values:	default, comverse	**Default:**	default

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.cid_src_priority.1`		
Description:	Set the desired caller ID source to be displayed on the incoming call screen.		
Values:	pai, rpid, from	**Default:**	pai

Setting:	`sip_account.x.cid_src_priority.2`		
Description:	Select the lower-priority caller ID source.		
Values:	pai, rpid, from	**Default:**	rpid

Setting:	`sip_account.x.cid_src_priority.3`
Description:	Select the lowest-priority caller ID source.
Values:	pai, rpid, from **Default:** from

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 (except when Call Forward Busy is enabled)
- 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

Setting:	`sip_account.x.dtmf_payload_type`
Description:	Set the configurable RTP payload type for in-call DTMF.
Values:	96–127 **Default:** 101

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 idle screen, 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.share_line_enable`
Description:	Sets the account type for account x. If the shared line type is enabled, multiple VSP861 desksets can be configured with shared line appearances.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`sip_account.x.access_code_page`
Description:	Sets the paging feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_code_park_call`
Description:	Sets the Call Park feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_code_retrieve_parked_call`
Description:	Sets the retrieve parked call feature access code for account x.
Values:	Text string **Default:** Blank

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.access_code_call_waiting_on`
Description:	Sets the Call Waiting ON feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_code_call_waiting_off`
Description:	Sets the Call Waiting OFF feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_code_group_call_pickup`
Description:	Sets the Group Call Pickup feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_code_direct_call_pickup`
Description:	Sets the Direct Call Pickup feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_sf_on`
Description:	Sets the Comverse Secretarial Filtering ON feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_sf_off`
Description:	Sets the Comverse Secretarial Filtering OFF feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_hg_on`
Description:	Sets the Comverse Hunt Group ON feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.access_hg_off`
Description:	Sets the Comverse Hunt Group OFF feature access code for account x.
Values:	Text string **Default:** Blank

Setting:	`sip_account.x.blf_list_uri`
Description:	Sets the Busy Lamp Field (BLF) list URI for account x. The device will retrieve the list from this location.
Values:	SIP URI text string **Default:** Blank

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 VSP861 uses the account x user ID for MWI subscription.
Values:	SIP URI text string **Default:** Blank

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

hs_settings Module: Handset Settings

The Handset Settings allow you to configure settings for the cordless accessories that are registered to the deskset. For more information on registering cordless accessories, see the VSP861 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

Setting:	`hs_settings.x.headset_us_pin_code`
Description:	Sets the new 4-digit PIN for headset registration/deregistration.

Values:	4-digit number	**Default:**	1590

MAC-specific configuration file settings

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

Values:	Text string	**Default:**	HANDSET

network Module: Network Settings

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

General configuration file settings

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.vlan.pc.enable`
Description:	Enables or disables the PC port VLAN.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`network.vlan.pc.id`
Description:	Sets the PC port VLAN ID.
Values:	0–4095 **Default:** 0

Setting:	`network.vlan.pc.priority`
Description:	Sets the PC port priority.
Values:	0–7 **Default:** 0

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

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 VSP861

Setting:	`network.user_class`
Description:	Sets the user class for DHCP option 77.
Values:	Text string

Default: Vtech Vesa VSP861

Setting:	`network.pc_port.enable`
Description:	Enable or disable the PC port to operate in hub/switch mode (depending on the Enable PC Port Mirroring setting).
Values:	0 (disabled), 1 (enabled)

Default: 1

Setting:	network.pc_port.mirroring.enable
Description:	When the PC port is enabled, enable PC Port Mirroring to set the port to operate in hub mode (network traffic on the WAN port is reflected in the PC port). When Port Mirroring is not enabled, the port operates in switch mode.

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

MAC-specific configuration file settings

Setting:	network.ip.mode
Description:	Sets the IPv4 network mode.

Values:	disable, dhcp, static, pppoe	Default:	dhcp

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

Setting:	`network.ip.manually_configure_dns`
Description:	Enable or disable manual DNS configuration.
Values:	0 (disable), 1 (enable) **Default:** 0

Setting:	`network.ip.pppoe.service_name`
Description:	If IPv4 mode is PPPoE, enter the name of the applicable PPPoE provider, in case more than one is available.
Values:	Text string **Default:** Blank

Setting:	`network.ip.pppoe.username`
Description:	If IPv4 mode is PPPoE, enter your PPPoE account username.
Values:	Text string **Default:** Blank

Setting:	`network.ip.pppoe.access_password`
Description:	If IPv4 mode is PPPoE, enter your PPPoE account password.
Values:	Text string **Default:** Blank

Setting:	`network.ipv6.mode`
Description:	Set the IPv6 network mode, depending on how the device will be assigned an IP address.
Values:	disable, auto, static **Default:** disable

Setting:	`network.ipv6.prefix`
Description:	When IPv6 mode is static, enter the IPv6 address prefix length.
Values:	0–128 **Default:** 64

Setting:	`network.ipv6.gateway_addr`
Description:	When IPv6 mode is static, enter the default gateway address.
Values:	Text string (IPv6) **Default:** Blank

Setting:　　　`network.ipv6.dns1`

Description:　If manual DNS configuration is enabled, enter the address for the primary DNS server.

Values:　　　Text string (IPv6)　　　**Default:**　　　Blank

Setting:　　　`network.ipv6.dns2`

Description:　If manual DNS configuration is enabled, enter the address for the secondary DNS server.

Values:　　　Text string (IPv6)　　　**Default:**　　　Blank

Setting:　　　`network.ipv6.manually_configure_dns`

Description:　Enable or disable manual DNS configuration for IPv6.

Values:　　　0 (disable), 1 (enable)　　　**Default:**　　　0

Setting:　　　`network.vpn.enable`

Description:　If manual DNS configuration is enabled, enter the address for the secondary DNS server.

Values:　　　Text string (IPv6)　　　**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 VSP861.

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

Setting:	`provisioning.click_to_dial`
Description:	Enables or disables "click to dial" functionality for directory entries on the WebUI.
Values:	0 (disabled), 1 (enabled) **Default:** 1

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:** https://et.vtechphones.com/rg2

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 VSP861 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 VSP861 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
- network.ip.pppoe.access_password
- tr069.acs.access_password
- tr069.connection_request.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

security Module: Security Settings

The Security settings enable you to hide PIN numbers during call operation. There are two different types of PIN masking available:

1. Hide DTMF digits: When Hide DTMF is enabled, PIN numbers entered during an Active Call are automatically masked out.

2. Password Dial: When Password Dial is enabled, PIN numbers entered as part of the dial string are hidden. For example, when entering numbers in Pre-Dial or Dial mode, PIN numbers are automatically masked out.

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

Setting:	`security.hide_dtmf_enable`
Description:	Enable or disable masking all DTMF digits entered during an Active Call.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`security.hide_dtmf_delay_enable`
Description:	Enable to add a one-second delay before DTMF digits are masked. By default, the digits are masked immediately.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`security.pwd_dial_enable`
Description:	Enable to hide PIN numbers entered as part of the dial string.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`security.pwd_dial_delay_enable`
Description:	Enable to add a one-second delay before PIN numbers are masked. By default, the PIN number is masked immediately.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`security.pwd_dial_prefix`
Description:	Enter the prefix that serves as an indicator that the next x digits are masked (x being equal to the Password Dial Length).
Values:	Text string **Default:** Blank

Setting:	`security.pwd_dial_length`
Description:	Enter the PIN number length. All digits within this length are masked. Any digits beyond this length are not masked.
Values:	1–32 **Default:** 1

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 VSP861.

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

Setting:	`time_date.date_format`		
Description:	Sets the format for displaying the date.		
Values:	DD/MM/YY, MM/DD/YY, YY/MM/DD	**Default:**	DD/MM/YY

Setting:	`time_date.24hr_clock`		
Description:	Enables or disables 24-hour clock.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

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,   **Default:**   America/New_York
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

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, **Default:** Sunday Wednesday, Thursday, Friday, Saturday

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, **Default:** Sunday Wednesday, Thursday, Friday, Saturday

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 **Default:** 2016-03-01T12:00:00 <hour>:<minute>:<second>

log Module: System 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:	IPv4, IPv6 or FQDN **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 VSP861.

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

Setting:	`remoteDir.ldap_enable`
Description:	Enables or disables the VSP861 deskset'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 VSP861 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 VSP861 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 VSP861 searches the LDAP directory for the incoming call number. If the number is found, the VSP861 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

Setting:	`remoteDir.broadsoft_enable`		
Description:	Enables or disables the Broadsoft phonebook.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	`remoteDir.broadsoft_display_name`		
Description:	Sets the Broadsoft Phonebook display name.		
Values:	Text string	**Default:**	Blank

Setting:	`remoteDir.broadsoft_server`		
Description:	Sets the Broadsoft Phonebook IP address.		
Values:	Text string	**Default:**	Blank

Setting:	`remoteDir.broadsoft_port`		
Description:	Sets the Broadsoft Phonebook port.		
Values:	1–65535	**Default:**	0

Setting:	`remoteDir.broadsoft_user_name`		
Description:	Sets the Broadsoft Phonebook authentication user name.		
Values:	Text string	**Default:**	Blank

Setting:	`remoteDir.broadsoft_access_password`		
Description:	Sets the Broadsoft Phonebook authentication password.		
Values:	Text string	Default:	Blank

Setting:	`remoteDir.broadsoft_dir_type`		
Description:	Sets the Broadsoft Phonebook directory type.		
Values:	Group, GroupCommon, Enterprise, EnterpriseCommon, Personal	Default:	Group

Setting:	`remoteDir.ldap_check_certificate`		
Description:	Enables or disables accepting only a trusted LDAP certificate.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	`remoteDir.broadsoft_check_certificate`		
Description:	Enables or disables accepting only a trusted Broadsoft certificate.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	`remoteDir.xml.x.name`		
Description:	Sets the name of the directory as it will appear on the phone's Directory list. For this and following parameters, x is the number of the XML directory (1–3).		
Values:	Text string	Default:	Blank

Setting:	`remoteDir.xml.x.uri`		
Description:	The location of the XML directory file, from which the phone will sync and retrieve directory entries.		
Values:	URI	Default:	Blank

Setting:	`remoteDir.xml.x.call_lookup_enable`		
Description:	Enables/disables the call lookup feature for incoming and outgoing calls.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	`remoteDir.xml.x.contact_entry_tag`		
Description:	Sets the tag name for directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY

Setting:	`remoteDir.xml.x.first_name_tag`		
Description:	Sets the first name tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NAME_FIRST

Setting:	`remoteDir.xml.x.last_name_tag`		
Description:	Sets the last name tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NAME_LAST

Setting:	`remoteDir.xml.x.work_number_tag`		
Description:	Sets the work number tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NUMBER_WORK

Setting:	`remoteDir.xml.x.mobile_number_tag`		
Description:	Sets the mobile number tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NUMBER_MOBILE

Setting:	`remoteDir.xml.x.other_number_tag`		
Description:	Sets the other number tag for a directory entry.		
Values:	Text string	**Default:**	DIR_ENTRY_NUMBER_OTHER

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.server_enable`
Description:	Enables or disables the availability of the phone's embedded WebUI.
Values:	0 (disabled), 1 (enabled) **Default:** 1

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

Setting:	`web.activeuri_enable`
Description:	Enables the Action URI feature, enabling remote activation of keys and features when a server sends an HTTP GET.
Values:	0 (disabled), 1 (enabled) **Default:** 0

trusted_ip Module: Trusted IP Settings

The trusted_ip settings provide enhanced security for the VSP861. When enabled, these settings can filter network traffic and reject any traffic from unauthorized sources.

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

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

Setting:	`trusted_ip.only_accept_allowed_ip`
Description:	Enables or disables using the Allowed IP list to filter network traffic. When enabled, all unsolicited IP traffic will be blocked unless it is from one of the trusted IP addresses on the "Allowed IP" list.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`trusted_ip.x.allow_ip`
Description:	Enter an IP address or address range for one instance of the "Allowed IP" list. x ranges from 1 to 10. See *"Trusted IP" on page 126* for more information.
Values:	Text string (IPv4 or IPv6, IP range in IPv4 or IPv6) **Default:** Blank

trusted_servers Module: Trusted Server Settings

The trusted_servers setting provides enhanced security for the VSP861. When enabled, this setting can filter network traffic and reject any traffic from unauthorized sources.

The trusted_servers setting follows the format: trusted_servers.[element].

The trusted_servers setting is included in the general configuration file.

Setting:	`trusted_servers.only_accept_sip_account_servers`
Description:	Enables or disables using each enabled account's Registration server, SIP server, Outbound Proxy server and Backup Outbound Proxy server as sources for trusted SIP traffic.
Values:	0 (disabled), 1 (enabled) **Default:** 0

user_pref Module: User Preference Settings

The user settings are accessible to the VSP861 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 settings (except for `user_pref.call_terminated.busy_tone_enable`) are exported when you manually export the configuration from the VSP861.

General configuration file settings

Setting:	`user_pref.account.x.ringer`
Description:	Sets the ring tone for account x.
Values:	1–10 **Default:** 1

Setting:	`user_pref.web_language`
Description:	Sets the language that appears on the WebUI.
Values:	en, en-GB, es-MX, es, fr-CA, **Default:** en fr, de, it, pt, nl, el, ru, tr, pl

Setting:	`user_pref.language`
Description:	Sets the language that appears on the device screen.
Values:	en, en-GB, es-MX, es, fr-CA, **Default:** en fr, de, it, pt, nl, el, ru, tr, pl

Setting:	`user_pref.notify.led.missed_call.enable`
Description:	Sets how the Message Waiting LED operates. When enabled, the LED turns on for missed calls and new messages. When disabled, the LED turns on for new messages only. **Note:** This setting is not available on the phone menu or WebUI.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	user_pref.text_input_option		
Description:	Sets the order and available language input options available when users edit or enter text on the LCD. **Note:** This setting is not available on the phone menu or WebUI, and applies to models sold and installed outside North America only.		
Values:	number,uc_western, lc_western,uc_ru,lc_ru, uc_el,lc_el	**Default:**	number,lc_western, uc_western

Setting:	user_pref.call_terminated.busy_tone_enable		
Description:	Enables the VSP861 to play a busy tone when the far-end party ends the call, or when a network error condition (keep-alive failure) occurs.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	user_pref.account.x.diversion_display		
Description:	Enables or disables the display of diversion <name-addr> info (if available) for calls forwarded to account x.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	user_pref.blf_indication_option		
Description:	Configures the BLF LED behavior for different service providers. Two options are available, as described below.		

Option 1 behavior	**Option 2 behavior**
Registration Error: Blinking ORANGE (every 2 secs)	**Registration Error**: Off
Incoming call: Fast ORANGE flash	**Incoming call**: Fast ORANGE flash
Held call: Fast ORANGE flash*	**Held call**: Fast ORANGE flash*
Active call: Steady ORANGE	**Active call**: Steady ORANGE
Idle: Off	**Idle**: Steady GREEN
* behavior applies only to certain servers.	

Values:	1, 2	**Default:**	1

Setting:	user_pref.quick_transfer		
Description:	Sets transfer options for Quick Dial and BLF Programmable keys during an active call.		
Values:	new_call, blind, attended	**Default:**	new_call

MAC-specific configuration file settings

Setting:	`user_pref.backlight_timeout`
Description:	Sets the backlight timeout in seconds.
Values:	10–60 **Default:** 30

Setting:	`user_pref.audio_mode`
Description:	Sets the default audio mode.
Values:	speaker, headset **Default:** speaker

Setting:	`user_pref.hold_reminder.enable`
Description:	Enables or disables audible hold reminder.
Values:	0 (disabled), 1 (enabled) **Default:** 1

Setting:	`user_pref.hold_reminder.interval`
Description:	Sets the interval for the audible hold reminder in seconds.
Values:	10–300 **Default:** 30

Setting:	`user_pref.call_waiting.tone_enable`
Description:	Enables or disables the call waiting tone.
Values:	0 (disabled), 1 (enabled) **Default:** 1

Setting:	`user_pref.call_waiting.tone_interval`
Description:	Sets the interval for the call waiting tone in seconds.
Values:	10–60 **Default:** 30

Setting:	`user_pref.call_waiting.mode`
Description:	Enables or disables rejecting calls if already on a call.
Values:	0 (disabled), 1 (enabled) **Default:** 1

Setting:	`user_pref.lcd_contrast`
Description:	Sets the LCD contrast on the VSP861.
Values:	1–7 **Default:** 4

Setting:	user_pref.backlight		
Description:	Sets the backlight brightness level.		
Values:	off, low, medium, high	**Default:**	high

Setting:	user_pref.idle_backlight		
Description:	Sets the backlight brightness level when the VSP861 is idle.		
Values:	off, low, medium, high	**Default:**	off

Setting:	user_pref.absent_timeout		
Description:	Sets the absent timeout (the interval after going off hook with no action taken) in seconds. After the absent timeout, the phone returns to idle mode.		
Values:	10–60	**Default:**	30

Setting:	user_pref.speaker_volume		
Description:	Sets the speakerphone volume.		
Values:	1–9	**Default:**	5

Setting:	user_pref.headset_volume		
Description:	Sets the headset volume.		
Values:	1–9	**Default:**	5

Setting:	user_pref.handset_volume		
Description:	Sets the corded handset volume.		
Values:	1–9	**Default:**	5

Setting:	user_pref.key_beep_enable		
Description:	Enables or disables key beeps on the VSP861.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

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 .

General configuration file settings

Setting:	`call_settings.account.x.call_completion_enable`
Description:	Enables or disables the Call Completion for Busy Subscribers (CCBS) feature. The feature notifies users when a previously busy number is available and asks them whether they wish to call the number back.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`call_settings.account.x.call_completion_alert_enable`
Description:	Enables or disables an audible alert (similar to a hold reminder alert tone) if the user is on another call when the auto redial interval expires.
Values:	0 (disabled), 1 (enabled) **Default:** 1

Setting:	`call_settings.account.x.auto_redial_interval`
Description:	Sets the countdown timer (in seconds) until the user is prompted for the next dialing attempt.
Values:	1–300 **Default:** 30

Setting:	`call_settings.account.x.auto_redial_repeat`
Description:	Sets how many auto redial attempts are made.
Values:	1–30 **Default:** 10

MAC-specific configuration file settings

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.dnd_incoming_calls`
Description:	Sets whether incoming calls are shown or rejected when DND is on for account x.
Values:	show, reject **Default:** reject

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

Setting:	`call_settings.missed_call_alert_enable`
Description:	Enables or disables missed call alerts.
Values:	0 (disabled), 1 (enabled) **Default:** 1

Setting:	`call_settings.hotline_enable`
Description:	Enables or disables the hotline feature.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`call_settings.hotline_account`
Description:	Sets the account used for dialing the hotline number.
Values:	0– **Default:** 0 (default account)

Setting:	`call_settings.hotline_number`
Description:	Sets the number dialed by the hotline feature.
Values:	Text string **Default:** Blank

Setting:	`call_settings.hotline_delay`
Description:	Sets the delay (in seconds) between the phone going off hook and the hotline number being dialed.
Values:	0–10 **Default:** 0

Setting:	`call_settings.account.x.unconditional_auto_answer_enable`
Description:	Enables or disables unconditional Auto Answer. Auto Answer allows a deskset or conference phone to automatically answer incoming calls to that account without user intervention. An auto answer tone will sound.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`call_settings.account.x.unconditional_auto_answer_delay`
Description:	Sets the delay before the phone auto answers a call.
Values:	0–30 **Default:** 2

Setting:	`call_settings.account.x.unconditional_auto_answer_mute_on_ans`
Description:	Enables or disables muting the mic upon auto answering.
Values:	0 (disabled), 1 (enabled) **Default:** 0

pfk Module: Programmable Feature Key Settings

The programmable feature key (PFK) settings store the data associated with each programmable key. On ErisTerminal desksets, you can program the programmable feature keys.

All the programmable feature key settings are included in the general configuration file.

Programmable Feature Keys

The programmable feature key settings follow the format: pfk.x.[element], where x is the programmable feature key ID, ranging from 1 to 30.

Setting:	`pfk.x.feature`
Description:	Assigns a feature to PFK x.

Values:	unassigned, line, dir, call log, redial, messages, dnd, dnd all, cfwd all, cfwd busy, cfwd no answer, quick dial, busy lamp field, acd, page, multicast page, park call, retrieve parked call, in call dtmf, callback, group call pickup, direct call pickup, prefix_dial, chp, hg, sf, lock_key, flash, xml app	**Default:**	See *"Programmable Feature Keys" on page 15*.

Setting:	`pfk.x.quick_dial`
Description:	Sets the quick dial string to use if quick dial is assigned to PFK x.

Values:	Text string (SIP URI)	**Default:**	Blank

Setting:	`pfk.x.blf`
Description:	Sets the BLF string to use if Busy Lamp Field is assigned to PFK x.

Values:	Text string (SIP URI)	**Default:**	Blank

Setting:	`pfk.x.incall_dtmf`
Description:	Sets the DTMF string if In-call DTMF is assigned to PFK x.

Values:	Text string (SIP URI)	**Default:**	Blank

Setting: `pfk.x.multicast_zone`

Description: Sets the multicast paging zone if multicast page is assigned to PFK x.

Values: 1–10   **Default:** Blank

Setting: `pfk.x.account`

Description: Sets the SIP account used for the assigned feature (if applicable).

Values: 1–8   **Default:** 1

Setting: `pfk.x.page_destination`

Description: If required by your service provider, enter a page destination number. The target number for the outgoing page will be formed by concatenating Paging feature access code of the selected account and the PFK page destination value.

Values: text string   **Default:** blank

Setting: `pfk.x.park_destination`

Description: If required by your service provider and `sip_account.x.park_variant` setting, enter a value for the park "orbit" or extension.

Values: text string   **Default:** blank

Setting: `pfk.x.park_retrieval_source`

Description: If required by your service provider and `sip_account.x.park_variant` setting, enter a value for the park "orbit" or extension.

Values: text string   **Default:** blank

Setting: `pfk.x.prefix`

Description: Enter a prefix to be dialed (hidden from the user) when the key is pressed. The prefix is added to any user-entered digits. **%N** can be used for substitution of user-entered digits. For example, ***71%N#** uses [*71] + [user-entered digits] + [#] as the outgoing dialing string.

Values: text string   **Default:** blank

Setting:	`pfk.x.call_handling_profile`
Description:	If pfk.x.feature is chp, enter the string of the call handling profile that the pfk LED will indicate.
Values:	text string **Default:** blank

Setting:	`pfk.x.call_handling_profile_set_code`
Description:	If pfk.x.feature is chp, enter the call handling profile FAC and profile index number to activate the profile.
Values:	text string **Default:** blank

Setting:	`pfk.x.hunt_group`
Description:	If pfk.x.feature value is hg, enter the hunt group extension number assigned for this pfk.
Values:	text string **Default:** blank

Setting:	`pfk.x.secretarial_filtering`
Description:	If pfk.x.feature value is sf, enter the manager's extension number assigned for this pfk
Values:	text string **Default:** blank

Setting:	`pfk.x.xml_uri`
Description:	If pfk.x.feature is xml app, enter the URI to fetch the XML application to be executed.
Values:	text string **Default:** blank

Setting:	`pfk.x.direct_pickup`
Description:	If pfk.x.feature is direct call pickup, enter the Direct Call Pickup feature access code (FAC).
Values:	text string **Default:** blank

application Module: Application Shortcuts

The application shortcut settings store the data associated with each application shortcut displayed on the three pages of the Home screen.

Application Shortcuts

The application shortcut settings follow the format: application.x.[element], where x is the application shortcut key ID, ranging from 1 to 30.

Setting:	`application.x.feature`
Description:	Assigns a feature to application shortcut.

Values:	unassigned, new call, redial, dir, call center, settings, status, messages, dnd all, call log, cfwd all, callback, blacklist, pfk, line, multicast page, select line, select zone, call recording, select default line	**Default:**	app 1: new call app 2: call center app 3: pfk app 4: settings app 5: messages app 6: dir app 7: dnd all app 8: cfwd all app 9: call recording app 10: call log app 11: select line app 15: status app 16: select zone app 17: blacklist app 20: redial app 12-14, 18-19, 21-30: unassigned

Setting:	`application.x.account`
Description:	Sets the SIP account used for the assigned feature (if applicable).

Values:	1–8	**Default:**	1

Setting:	`application.x.multicast_zone`
Description:	Sets the multicast paging zone if multicast page is assigned to application shortcut.

Values:	1–10	**Default:**	Blank

speed_dial Module: Speed Dial Settings

The speed dial key settings configure the dial pad keys for speed dialing pre-programmed phone numbers. When configured, the VSP861 user can press and hold a dial pad key to dial a programmed phone number.

The speed dial key settings follow the format speed_dial.x.[element], where x is the dial pad key, ranging from 1 to 0 (with 0 being the "0" OPER key).

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

Setting:	`speed_dial.x.name`
Description:	Sets the name associated with the phone number for dial pad key x. The name is visible on the VSP861 screen.
Values:	Text string **Default:** Blank

Setting:	`speed_dial.x.number`
Description:	Sets the phone number that dial pad key x dials when pressed and held.
Values:	Text string (SIP URI) **Default:** Blank

Setting:	`speed_dial.x.account`
Description:	Sets the SIP account used for dialing when dial pad key x is pressed and held.
Values:	0– (0 is the default account) **Default:** 0

audio Module: Audio Settings

The audio settings include jitter buffer parameters and RTP port settings.

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

Setting:	`audio.x.jitter_mode`
Description:	Select the desired mode for the jitter buffer: fixed (static) or adaptive. This setting depends on your network environment and conditions.
Values:	fixed, adaptive **Default:** adaptive

Setting:	`audio.x.fixed_jitter.delay`
Description:	When in fixed jitter buffer mode, set the delay (in ms) desirable to provide good audio quality with the minimal possible delay.
Values:	30–500 **Default:** 70

Setting:	`audio.x.adaptive_jitter.min_delay`
Description:	When in adaptive jitter buffer mode, set the minimum delay (in ms) desirable to maintain data packet capture and audio quality.
Values:	20–250 **Default:** 60

Setting:	`audio.x.adaptive_jitter.target_delay`
Description:	When in adaptive jitter buffer mode, set the target delay (in ms) desirable to provide good audio quality with the minimal possible delay.
Values:	20–500 **Default:** 80

Setting:	`audio.x.adaptive_jitter.max_delay`
Description:	When in adaptive jitter buffer mode, set the maximum delay (in ms) desirable to maintain data packet capture and audio quality.
Values:	180–500 **Default:** 240

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

Setting: `audio.x.rtp.port_end`

Description: Sets the Local RTP port range end.

Values: 1–65535   **Default:** 19000

Setting: `audio.x.rtcp_xr.enable`

Description: Enables or disables reporting of RTCP XR via SIP to a collector server. RTP Control Protocol Extended Reports (RTCP XR) are used for voice quality assessment and diagnostics.

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

ringersetting Module: Distinctive Ringer Settings

The distinctive ringer settings configure the distinctive ringer feature. For more information, see *"Ringer Settings" on page 78*. You can configure up to 8 instances of the distinctive ringer feature.

The ringer setting parameters follow the format ringersetting.x.[element], where x is the instance of the setting, ranging from 1 to 8.

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

Setting:	`ringersetting.x.ringer_text`
Description:	Enter the text that will match the "info" parameter and play the ringer tone. The matching of the "info" parameter and ringer_text setting is case sensitive.

Values:	Text string in the format **ringerx** (e.g., ringer1)	**Default:**	Blank

Setting:	`ringersetting.x.ringer_type`
Description:	Select the desired ring tone for ringer setting x.

Values:	1–10	**Default:**	1

call_record Module: Call Recording Settings

The call recording settings configure call recording for the VSP861. Ensure that a microSD is also inserted into the unit.

All the call recording settings are included in the general configuration file.

Setting:	`call_record.enable`
Description:	Enables call recording on the deskset.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`call_record.tone_enable`
Description:	Enables a call record tone, to be played over the line when recording begins and ends.
Values:	0 (disabled), 1 (enabled) **Default:** 1

file Module: Imported File Parameters

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

- Contact lists

- Custom logos

- Security certificates

Certificates can be added via provisioning. There are two types of certificate:

- Trusted: Trusted Certificates are for server authentication with secured HTTP transaction in the following applications: SIP signaling, Provisioning, Firmware, LDAP directory service, and Broadsoft directory service. Up to 20 trusted certificates can be installed.

- Device: A single Device Certificate can be uploaded so that other parties can authenticate the phone in the following cases:

  - When the phone acts as a web server for the user to manage configurations.
  - When the phone acts as a client for applications where HTTP is supported.

File parameter values are URLs that direct the VSP861 to the location of the file to be imported. The URL of certificate to be imported should follow the format <protocol>://<user>:<password>@<host>:<port>/<url-path>

None of these settings are exported when you manually export the configuration from the VSP861.

General configuration file settings

Setting:	`file.certificate.x.url`
Description:	URL to upload a trusted certificate file in pem or crt. It will be given index x and marked as unprotected. x ranges from 1 to 20.
Values:	Text string **Default:** Blank

Setting:	`file.protected_certificate.x.url`
Description:	URL to upload a trusted certificate file in pem or crt. It will be given index x and marked as protected. x ranges from 1 to 20.
Values:	Text string **Default:** Blank

Setting: `file.certificate.trusted.url`

Description: URL to upload a trusted certificate file in pem or crt. It will be given the first available index and marked as unprotected.

Values: Text string   **Default:**   Blank

Setting: `file.protected_certificate.trusted.url`

Description: URL to upload a trusted certificate file in pem or crt. It will be given the first available index and marked as protected.

Values: Text string   **Default:**   Blank

Setting: `file.protected_certificate.custom_device.url`

Description: URL to upload a custom device certificate to override the factory installed device certificate.

Values: Text string   **Default:**   Blank

Setting: `file.action`

Description: Enables you to delete certain certificates.

- removecertificate_customdevice: remove the custom device certificate and resume the use of the factory installed device certificate
- removecertificate_allnonprotected: remove all non-protected trusted certificates
- removecertificate_all: remove the custom device certificate and all protected or non-protected trusted certificates

Enables you to delete a custom language from the WebUI, the deskset screens, or both.

Values: removecertificate_customdevice, removecertificate_allnonprotected, removecertificate_all removecustomlanguage_all, removecustomlanguage_webui, removecustomlanguage_desksetui   **Default:**   Blank

---

Setting:	`file.bootup_logo`		
Description:	URL of custom logo shown during bootup. For logo specifications, see *"Logo specifications" on page 21*. To restore the default "VTech" logo, set the value to %NULL in the configuration file. For example: `file.bootup_logo = %NULL`		
Values:	Text string	**Default:**	Blank

Setting:	`file.idle_logo`		
Description:	URL of custom logo shown on the idle screen. For logo specifications, see *"Logo specifications" on page 21*. To restore the default "VTech" logo, set the value to %NULL in the configuration file. For example: `file.bootup_logo = %NULL`		
Values:	Text string	**Default:**	Blank

Setting:	`file.language.deskset.url`		
Description:	URL of the Deskset UI Custom Language file to be imported.		
Values:	Text string	**Default:**	Blank

Setting:	`file.language.webui.url`		
Description:	URL of Web UI Custom Language file to be imported.		
Values:	Text string	**Default:**	Blank

Setting:	`file.vpn.advanced_config`		
Description:	URL of OpenVPN client configuration file. For more information, see *"VPN" on page 92*.		
Values:	Text string	**Default:**	Blank

MAC-specific configuration file settings

Setting:	`file.custom_ringer`		
Description:	Enter URI to WAV file for a custom ringer. The custom ringer replaces Ringtone 10 on Ringer tone menu. For more information about file format, see *"Custom Ringer" on page 68*. To restore the default "VTech" logo, set the value to %NULL in the configuration file. For example: `file.bootup_logo = %NULL`		
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

xml_app Module: XML App Settings

The VSP861 supports both push and pull server applications. The XML app settings allow you to enable "push" events and how they interact with the phone during calls.

The XML app settings are included in the general configuration file.

Setting:	`xml_app.http_push_enable`
Description:	Enable or disable HTTP push, which enables the phone to display XML objects that are "pushed" to the phone from the server via http/https POST or SIP NOTIFY.
Values:	0 (disabled), 1 (enabled) **Default:** 0

Setting:	`xml_app.push_during_call_enable`
Description:	Enable or disable the phone to display pushed XML objects during a call. Otherwise, the XML application is displayed after the call is over.
Values:	0 (disabled), 1 (enabled) **Default:** 0

system_event Module: Action URI Settings

You can enter Action URIs to allow the VSP861 to interact with a server application by using an HTTP GET request. The action URI triggers a GET request when a specified event occurs. Action URIs allow an external application to take control of the display when an event occurs. For more information, see *"Server Application" on page 81*.

All the Action URI settings are included in the general configuration file.

Setting:	`system_event.startup.action_uri`
Description:	Enter URI for GET request triggered at end of phone bootup.
Values:	Text string **Default:** Blank

Setting:	`system_event.registered.action_uri`
Description:	Enter URI for GET request triggered at end of line registration.
Values:	Text string **Default:** Blank

Setting:	`system_event.on_hook.action_uri`
Description:	Enter URI for GET request triggered when phone goes from active to idle.
Values:	Text string **Default:** Blank

Setting:	`system_event.off_hook.action_uri`
Description:	Enter URI for GET request triggered when phone goes into dial mode.
Values:	Text string **Default:** Blank

Setting:	`system_event.incoming_call.action_uri`
Description:	Enter URI for GET request triggered for incoming calls or call waiting events.
Values:	Text string **Default:** Blank

Setting:	`system_event.outgoing_call.action_uri`
Description:	Enter URI for GET request triggered when phone sends SIP INVITE message.
Values:	Text string **Default:** Blank

Setting:	`system_event.poll.action_uri`
Description:	Enter URI for GET request.
Values:	Text string **Default:** Blank

Setting:	`system_event.poll.interval`
Description:	Enter interval (in seconds) between poll.action_uri requests.
Values:	1–65535 **Default:** 3600

Setting:	`system_event.connected.action_uri`
Description:	Enter URI for GET request triggered when phone has active call or is paging.
Values:	Text string **Default:** Blank

Setting:	`system_event.registration_event.action_uri`
Description:	Enter URI for GET request triggered when the registration state changes.
Values:	Text string **Default:** Blank

tr069 Module: TR-069 Settings

The Broadband Forum's Technical Report 069 (TR-069) defines a protocol for remote management and secure auto-configuration of compatible devices. The TR-069 settings allow you to enable TR-069 and configure access to an auto-configuration server (ACS).

All the TR-069 settings are included in the general configuration file.

Setting: `tr069.enable`

Description: Enable/disable the TR-069 subsystem.

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

Setting: `tr069.acs.url`

Description: Enter the URL to the auto configuration server (ACS).

Values: Text string   **Default:** Blank

Setting: `tr069.acs.username`

Description: Enter user name for ACS authentication.

Values: Text string   **Default:** Blank

Setting: `tr069.acs.access_password`

Description: Enter password for ACS authentication.

Values: Text string   **Default:** Blank

Setting: `tr069.periodic_inform.enable`

Description: Enable/disable the phone sending Inform messages to the server.

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

Setting: `tr069.periodic_inform.interval`

Description: Set the interval (in seconds) between sending Inform messages.

Values: 1–65535   **Default:** 3600

Setting:	`tr069.connection_request.username`
Description:	Set the user name for authenticating the connection sent from the ACS.
Values:	Text string **Default:** Blank

Setting:	`tr069.connection_request.access_password`
Description:	Set the password for authenticating the connection sent from the ACS.
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 at least one element containing a string of 12 element attributes 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>: 0-2

<freq1>: 0-65535 (Hz)

<amp1>: -30-6 (dB)

<freq2>: 0-65535 (Hz)

<amp2>: -30-6 (dB)

<freq3>: 0 (for future development—modifying attribute has no effect)

<amp3>: 0 (for future development—modifying attribute has no effect)

<freq4>: 0 (for future development—modifying attribute has no effect)

<amp4>: 0 (for future development—modifying attribute has no effect)

<on duration>: 0-65535 (milliseconds)

<off duration>: 0-65535 (milliseconds)

<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 -22 0 0 0 0 0 0 500 0 1

Setting:	`tone.call_waiting_tone.element.x`		
Description:	Defines the call waiting tone element x (x = 2–5).		
Values:	Tone element string	**Default:**	Blank

Setting:	`tone.call_waiting_tone.num_of_repeat_all`		
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.		
Values:	0–65535	**Default:**	0

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 -22 0 0 0 0 0 0 300 0 1

Setting:	`tone.hold_reminder_tone.element.x`		
Description:	Defines the hold reminder tone element x (x = 2–5).		
Values:	Tone element string	**Default:**	Blank

Setting:	`tone.hold_reminder_tone.num_of_repeat_all`		
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.		
Values:	0–65535	**Default:**	0

Setting:	`tone.inside_dial_tone.num_of_elements`		
Description:	Sets the number of tone elements for the secondary dial tone (see *"Dial Plan" on page 54* for description and behavior).		
Values:	1–5	**Default:**	1

Setting:	`tone.inside_dial_tone.element.1`
Description:	Defines the secondary dial tone element 1.

Values:	Tone element string	**Default:**	2 440 -22 350 -22 0 0 0 0 65535 0 65535

Setting:	`tone.inside_dial_tone.element.x`
Description:	Defines the secondary dial tone element x (x = 2–5).

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

Setting:	`tone.inside_dial_tone.num_of_repeat_all`
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.

Values:	0–65535	**Default:**	0

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 -22 350 -22 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 -22 350 -22 0 0 0 0 65535 0 65535

Setting:	`tone.stutter_dial_tone.element.x`
Description:	Defines the stutter dial tone element x (x = 3–5).

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

Setting:	`tone.stutter_dial_tone.num_of_repeat_all`
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.

Values:	0–65535	**Default:**	0

Setting:	`tone.busy_tone.num_of_elements`
Description:	Sets the number of tone elements for the busy tone.

Values:	1–5	**Default:**	1

Setting:	`tone.busy_tone.element.1`
Description:	Defines the busy tone element 1.

Values:	Tone element string	**Default:**	2 480 -22 620 -22 0 0 0 0 500 500 65535

Setting:	`tone.busy_tone.element.x`
Description:	Defines the busy tone element x (x = 2–5).

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

Setting:	`tone.busy_tone.num_of_repeat_all`
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.

Values:	0–65535	**Default:**	0

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 -22 480 -22 0 0 0 0 2000 4000 65535

Setting:	`tone.ring_back_tone.element.x`
Description:	Defines the ringback tone element x (x = 2–5).

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

Setting:	`tone.ring_back_tone.num_of_repeat_all`
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.

Values:	0–65535	**Default:**	0

Setting:	`tone.dial_tone.num_of_elements`
Description:	Sets the number of tone elements for the dial tone.

Values:	1–5	**Default:**	1

Setting:	`tone.dial_tone.element.1`
Description:	Defines the dial tone element 1.

Values:	Tone element string	**Default:**	2 440 -22 350 -22 0 0 0 0 65535 0 65535

Setting:	`tone.dial_tone.element.x`
Description:	Defines the dial tone element x (x = 2–5).

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

Setting:	`tone.dial_tone.num_of_repeat_all`
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.

Values:	0–65535	**Default:**	0

Setting:	`tone.record_tone.num_of_elements`
Description:	Sets the number of tone elements for the record tone.

Values:	1–5	**Default:**	1

Setting: `tone.record_tone.element.1`

Description: Defines the record tone element 1.

Values: Record element string   **Default:**   1 770 -22 0 0 0 0 0 0 800 0 1

Setting: `tone.record_tone.element.x`

Description: Defines the record tone element x (x = 2–5).

Values: Record element string   **Default:**   Blank

Setting: `tone.record_tone.num_of_repeat_all`

Description: Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.

Values: 0–65535   **Default:**   0

Setting: `tone.congestion_tone.num_of_elements`

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

Values: 1–5   **Default:**   3

Setting: `tone.congestion_tone.element.1`

Description: Defines the dial tone element 1.

Values: Tone element string   **Default:**   1 950 -22 0 0 0 0 0 0 330 0 1

Setting: `tone.congestion_tone.element.2`

Description: Defines the dial tone element 2.

Values: Tone element string   **Default:**   1 1400 -22 0 0 0 0 0 0 330 0 1

Setting: `tone.congestion_tone.element.3`

Description: Defines the dial tone element 3.

Values: Tone element string   **Default:** 1 1800 -22 0 0 0 0 0 0 330 1000 1

Setting: `tone.congestion_tone.element.x`

Description: Defines the dial tone element x (x = 4–5).

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

Setting:	`tone.congestion_tone.num_of_repeat_all`
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.
Values:	0–65535 **Default:** 65535

Setting:	`tone.auto_answer_tone.num_of_elements`
Description:	Sets the number of tone elements for the auto answer tone.
Values:	1–5 **Default:** 1

Setting:	`tone.auto_answer_tone.element.1`
Description:	Defines the dial tone element 1.
Values:	Tone element string **Default:** 2 500 -22 800 -22 0 0 0 0 1000 0 1

Setting:	`tone.auto_answer_tone.element.x`
Description:	Defines the dial tone element x (x = 2–5).
Values:	Tone element string **Default:** Blank

Setting:	`tone.auto_answer_tone.num_of_repeat_all`
Description:	Sets the number of repeats of all elements in sequence; that is, repeating back to the first element.
Values:	0–65535 **Default:** 0

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 VSP861 and the WebUI.

Values: Text string   **Default:**   admin
(15 characters maximum)

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   **Default:**   user
(15 characters maximum)

page_zone Module: Paging Zone Settings

The paging zone settings allow you to define a maximum of 10 paging zones that the VSP861 can use for multicast paging.

The paging zone parameters (except for page_zone.call_priority_threshold) follow the format page_zone.x.[element], where x is the paging zone ID number, ranging from 1 to 10.

All the paging zone settings are included in the general configuration file.

Setting: `page_zone.x.name`

Description: Sets the paging zone name, which appears on VSP861 LCD for outgoing and incoming multicast pages. A maximum of 15 characters is allowed.

Values: Text string   **Default:**   Blank

Setting: `page_zone.x.multicast_address`

Description: Enter the multicast IP address that the VSP861 will monitor. The range of valid IP addresses is 224.0.0.0 to 239.255.255.255.

Values: IPv4, IPv6 or FQDN   **Default:**   Blank

Setting: `page_zone.x.multicast_port`

Description: Enter the multicast port associated with the multicast IP. The range of valid ports is 1 to 65535.

Values: 1–65535   **Default:**   Blank

Setting: `page_zone.x.accept_incoming_page`

Description: Enables or disables the VSP861 from receiving incoming multicast pages for that paging zone. If disabled, the VSP861 can make outgoing multicast pages only.

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

Setting: `page_zone.x.priority`

Description: Set the paging zone priority from 1 to 10. Zones with a priority higher than another zone can interrupt the lower-priority zone's active page.

Values: 1–10   **Default:**   5

Setting:	`page_zone.call_priority_threshold`
Description:	Set the call_priority_threshold. If the paging zone priority (page_zone.x.priority) is higher or equal to the call priority, then a multicast page can interrupt an active, dialing, or incoming call.
Values:	1–10 **Default:** 2

phonelock Module: Phone Lock Settings

The Phone Lock feature restricts certain hard keys and features unless the user enters a PIN code. For more information about phone lock modes, see *"Using the Phone Lock menu" on page 41*.

All the phone lock settings are part of the general configuration file.

Setting:	`phonelock.type`		
Description:	Sets the phone lock type.		
Values:	disabled, restricted_config, restricted_call, emergency_call_only	**Default:**	disabled

Setting:	`phonelock.pin`		
Description:	Sets the pin for unlocking the phone.		
Values:	4 to 15 digits	**Default:**	1234

Setting:	`phonelock.autolock_timeout`		
Description:	Sets the delay (in seconds) before the phone locks when idle.		
Values:	0 (disabled)–3600	**Default:**	0

Setting:	`phonelock.restricted_account`		
Description:	Sets the restricted account.		
Values:	0 (default)–4	**Default:**	0

C H A P T E R   6

TROUBLESHOOTING

If you have difficulty with your VSP861 deskset, 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.

Screen is blank.

■ Ensure power is connected. If powered by an AC adapter, check that the adapter is plugged into a wall socket and the VSP861 power jack. If powered by PoE, ensure that the network switch is providing power through the correct ports.

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

■ Ensure the headset is fully charged and in the charger. Remove and replace the headset in its charger before selecting **Register** on the VSP861.

■ Ensure the headset is not already registered to another phone. If it has been registered to another phone, deregister it.

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

■ Ensure the handset is fully charged and in the charger.

■ Ensure the handset is not already registered to another base. If it has been registered to another base, deregister it.

Pages are not received.

- The Page auto answer setting is set to Manual. Check the General Account Settings.

Calls are answered on the headset rather than the speakerphone after I press a Line key or Accept **to answer a call.**

- Change the audio mode from Headset to Speaker. On the VSP861 Home screen, press **Settings** > **User Settings** > **Audio** > **Audio mode**.

My computer can't connect to the network after plugging the Ethernet cable through the PC port.

- Make sure the VSP861 is connected to power. The PC port does not work when the VSP861 does not have power source or during a power outage.

- Make sure you plug the Ethernet cable connected to the router into the VSP861 Ethernet port and the Ethernet cable connected to the computer into the VSP861 PC port.

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 VSP861 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 telephone

■   Your VSP861 deskset contains sophisticated electronic parts, so you must treat it with care.

■   Avoid rough treatment.

■   Place the corded handset down gently.

■   Save the original packing materials to protect your VSP861 deskset if you ever need to ship it.

Avoid water

■   You can damage your VSP861 deskset if it gets wet. Do not use the corded handset in the rain, or handle it with wet hands. Do not install the VSP861 deskset 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 telephone

■   Your VSP861 deskset 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 VSP861 deskset 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 — VSP861 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.