



ErisTerminal® SIP DECT 4-Line base station VDP650

Administrator and Provisioning Manual



CONTENTS

Preface	7
Text Conventions	8
Audience	8
Related Documents	8
Introducing the VDP650	9
About the VDP650 4-Line base station	10
Quick Reference Guide	11
Network Requirements	13
VDP650 Configuration Methods	14
Using Shared Calls	15
Key System Emulation	17
Configuration Using the Phone Menus	19
Viewing the Main Menu	20
Using the Status menu	20
Viewing Line status	22
Using the Admin Settings Menu	23
Using the Network Setting menu	24
Using the Security menu	29
Using the Provisioning menu	29
Editing the handset PIN code	32
Using the WebUI	33
Using the Web User Interface (WebUI)	34
Status Page	37
System Status	37
Handset Status	38
System Pages	39
SIP Account Management	39
General Account Settings	39
Dial Plan	41
SIP Server Settings	42
Registration Settings	42

Outbound Proxy Settings	42
Backup Outbound Proxy Settings	43
Caller Identity Settings	43
Audio Settings	43
Quality of Service	45
Signaling Settings	45
Voice Settings	46
Feature Access Codes Settings	46
Voicemail Settings	48
NAT Traversal	49
Music on Hold Settings	49
Network Conference Settings	49
Session Timer	50
Jitter Buffer	50
Keep Alive	50
Call Settings.....	52
General Call Settings	52
Do Not Disturb.....	52
Call Forward	52
User Preferences.....	54
General User Settings.....	54
Handset Settings	54
Account Assignments.....	54
KeyLine Assignments.....	56
Repeater Mode	58
Handset Name	59
Server Application.....	59
Action URI Syntax	59
Action URI	61
XML Push Settings.....	63
Network Pages	64
Basic Network Settings.....	65
Basic Network Settings	65
Advanced Network Settings.....	67
VLAN.....	67
LLDP-MED	68
802.1x	68
VPN.....	69
Contacts Pages	70
Base Directory	70
Create Base Directory Entry	72
Directory Import/Export	73
Blacklist	73
Create Blacklist Entry.....	75
Blacklist Import/Export	76
LDAP	77
LDAP Settings.....	77
Remote XML.....	80
Remote XML Directory Format	80

Servicing Pages.....	82
Reboot.....	82
Time and Date	82
Time and Date Format	83
Network Time Settings	83
Time Zone and Daylight Savings Settings	83
Manual Time Settings.....	84
Custom Language	85
Firmware Upgrade.....	86
Firmware Server Settings.....	86
Manual Firmware Update and Upload	88
Updating a Cordless Handset/Deskset	88
Provisioning	91
Provisioning Server.....	92
Plug-and-Play Settings.....	92
DHCP Settings	93
Resynchronization.....	93
Import Configuration.....	95
Export Configuration	95
Reset Configuration	96
Security.....	97
Passwords.....	97
Web Server	98
Trusted Servers	99
Trusted IP	100
Certificates.....	101
Device Certificate	101
Trusted Certificate	102
TR-069 Settings.....	103
System Logs	104
Syslog Settings	104
Network Trace	105
Download Log	105
Provisioning Using Configuration Files.....	106
The Provisioning Process.....	107
Resynchronization: configuration file checking.....	108
VDP650 restart	108
Configuration File Types.....	109
Data Files.....	110
Configuration File Tips and Security	111
Clearing parameters with %NULL in configuration file	111
Guidelines for the MAC-Specific configuration file.....	111
Securing configuration files with AES encryption	112
Configuration File Parameter Guide.....	114
"sip_account" Module: SIP Account Settings	116
General configuration file settings	116

MAC-specific configuration file settings	124
"hs_settings" Module: Handset Settings	128
General configuration file settings	128
MAC-specific configuration file settings	132
system Module: System settings	134
General configuration file settings	134
"network" Module: Network Settings	135
General configuration file settings	135
MAC-specific configuration file settings	137
"provisioning" Module: Provisioning Settings	140
General configuration file settings	140
MAC-specific configuration file settings	143
"time_date" Module: Time and Date Settings	145
"log" Module: Log Settings	149
"remoteDir" Module: Remote Directory Settings	150
"web" Module: Web Settings	155
"trusted_ip" Module: Trusted IP Settings	156
"trusted_servers" Module: Trusted Server Settings	157
"user_pref" Module: User Preference Settings	158
"call_settings" Module: Call Settings	159
"audio" Module: Audio Settings	161
"file" Module: Imported File Settings	163
General configuration file settings	163
MAC-specific configuration file settings	165
"tr069" Module: TR-069 Settings	166
"tone" Module: Tone Definition Settings	168
"profile" Module: Password Settings	172
General configuration file settings	173
MAC-specific configuration file settings	173
Troubleshooting	174
Common Troubleshooting Procedures	174
Appendixes	176
Appendix A: Maintenance	176
Appendix B: GPL License Information	177

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 VDP650 SIP DECT 4-Line base station with software version 1.0.0.7 or newer. See *"Using the Status menu" on page 20* for instructions on checking the software version on the VDP650. Please read this manual before installing the product.

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

Model number: VDP650

Type: Small-to-medium business SIP-endpoint base station

Serial number: _____

Purchase date: _____

Place of purchase: _____



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

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

Text Conventions

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

Table 1. Description of Text Conventions

Text Format	Description
Screen	Identifies text that appears on a device screen or a WebUI page in a title, menu, or prompt.
HARD KEY or DIAL-PAD KEY	Identifies a hard key, including the dial-pad keys.
CallFwd	Identifies a soft key.
 NOTE	Notes provide important information about a feature or procedure. Example of a Note.
 CAUTION	<i>A caution means that loss of data or unintended circumstances may result.</i> 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 VDP650 SIP DECT 4-Line base station becomes certified for IP PBX equipment or services, VTech may publish interop guides for those specific services. The interop guides will recommend second-party devices and settings, along with VDP650-specific configurations for optimal performance with those services. For the latest updates, visit our website at businessphones.vtech.com.

Related Documents

The **VDP650 Quick Start Guide** contains a quick reference guide to the VDP650 external features and brief instructions on connecting the VDP650 to a working IP PBX system.

The **VDP650 User Guide** contains a quick reference guide, full installation instructions, instructions for making and receiving calls, and a guide to all user-configurable settings.

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

CHAPTER 1

INTRODUCING THE VDP650

This administrator and provisioning guide contains detailed instructions for configuring the VDP650 SIP DECT 4-Line base station. Please read this guide before attempting to configure the VDP650.

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 VDP650 4-Line base station” on page 10](#)*
- *[“Quick Reference Guide” on page 11](#)*
- *[“Network Requirements” on page 13](#)*
- *[“VDP650 Configuration Methods” on page 14](#)*

About the VDP650 4-Line base station

The VTech VDP650 SIP DECT 4-Line base station with VDP651 cordless handset is a cordless business phone system designed to work with popular SIP telephone (IP PBX) equipment and services. Once you have ordered and configured your SIP equipment or service, the VDP650 and cordless accessories enable you to make and receive calls as you would with any other business phone.

The VDP650 4-Line base station features include:

- Up to 8 SIP account registrations
- Up to 4 active SIP sessions (across all handsets and cordless desksets)
- Registration of up to 10 DECT cordless handsets
- Shared call usage (held call pick up, call barge in to conference) on single SIP account among multiple users
- Power over Ethernet
- Handset locator
- 1,000-entry base directory with entries shared on all registered handsets and desksets

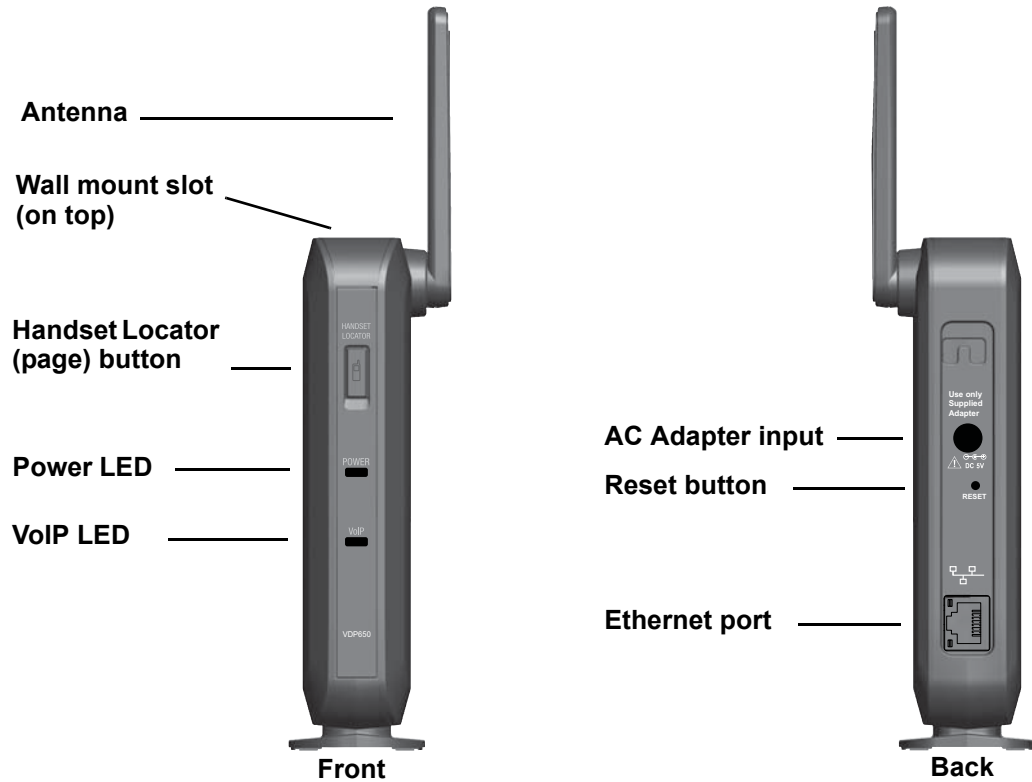
The VDP651 cordless handset features include:

- 4 dedicated Line keys for Key System experience
- Backlit Liquid Crystal Display
- Speakerphone, hold, intercom and mute capability
- Corded headset jack
- 3-way conferencing
- 200-entry call history
- 500-entry local directory

You can configure the VDP650 using the menus on the VDP651 handset, a browser-based interface called the WebUI, or an automatic provisioning process (see [“Provisioning Using Configuration Files” on page 106](#)). The WebUI enables you to configure the VDP650 using a computer that is connected to the same Local Area Network. The WebUI resides on the VDP650, and may get updated with firmware updates.

Quick Reference Guide

The external features of the VDP650 4-Line base station and handset are described below.





Network Requirements

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

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

The VDP650 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 VDP650 4-Line base stations so that IP addresses can be auto-assigned. In most cases, your network router will have a DHCP server. By default, the VDP650 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 VDP650. You can assign a static IP address using the VDP650 menu. To assign a static IP, go to **Admin settings > Network setting > Set static IP**. If you do not have a DHCP server or do not manually assign static IPs, you will not be able to access the WebUI and/or enable automatic time updates from an NTP server.

A DNS server is recommended to resolve the path to the Internet and to a server for firmware and configuration updates. If necessary, the system administrator can also download upgrade files and use the WebUI to update the VDP650 firmware and/or configuration settings manually.

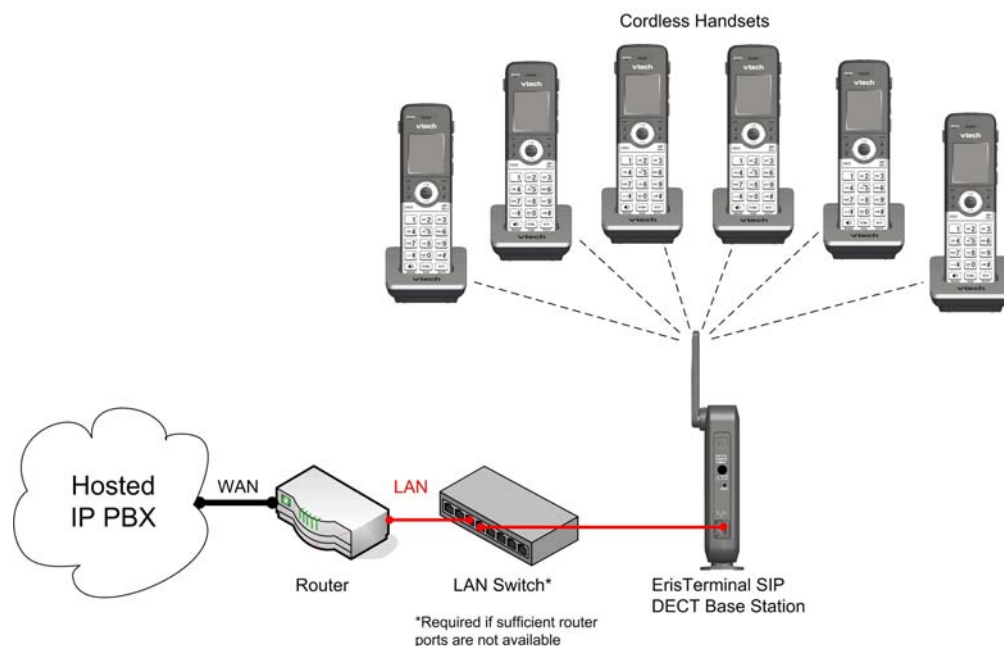


Figure 1. VDP650 Installation Example

VDP650 Configuration Methods

You can configure the VDP650 using one of the following methods:

- From the VDP651 handset, using the handset menus. The VDP651 menus are best suited to configuring a few settings, perhaps after the initial setup has been done. For administrators, the settings available on the VDP651 menus include network settings, account settings, and provisioning settings. See [“Using the Admin Settings Menu” on page 23](#). Many of the settings accessible on the VDP651 are most useful for end users. Through the menu, they can customize the screen appearance, sounds, and manage calls. For more information, see the VDP650/VDP651 User Guide.
- The Web User Interface, or WebUI, which you access using your Internet browser. See [“Using the WebUI” on page 33](#). The browser-based interface is easy to navigate and best suited to configuring a large number of VDP650 settings at once. The WebUI gives you access to every setting required for configuring a single device. You can enter service provider account settings on the WebUI, assign accounts to handsets, and set up provisioning, which will allow you to automatically and remotely update the VDP650 after initial configuration.
- Provisioning using configuration files. Working with configuration files allows you to configure the device at regular intervals. There are several methods available to enable the VDP650 to locate and upload the configuration file. For example, you can enable the VDP650, 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 VDP650 automatically downloads the file and applies the new settings. For more information, see [“Provisioning Using Configuration Files” on page 106](#).

Using Shared Calls

Your system allows shared calls usage among multiple handset users on a SIP account.

Incoming calls on an account can alert multiple handsets and be answered by any one of them. Multiple handsets can share an account for outgoing calls. This can be achieved via Account Assignments. For more details, see [“Account Assignments” on page 54](#).

Typical call sharing operations like held call pick up and barge-in conference among handset users can be achieved via KeyLine Assignments. For more details, see [“KeyLine Assignments” on page 56](#).

Each "KeyLine" number, when assigned to a shared call, behaves as a virtual "Line" number allowing easy, yet unique reference across multiple handset users.

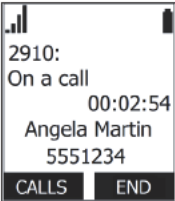
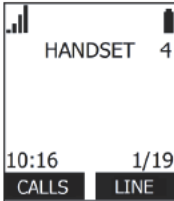

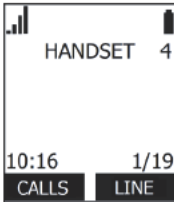
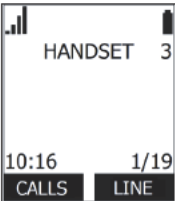

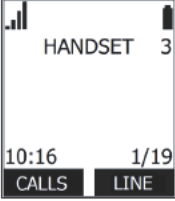
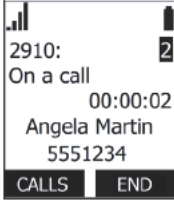
Using our default configuration for KeyLine as an example, any incoming/outgoing call on account 1 will get assigned a KeyLine number. The lowest unoccupied KeyLine number will typically be assigned first.

Please see the following scenarios to see how the KeyLine number can be utilized among users via the Call List.

Example - barging in a shared call:

	Alice's handset	Bob's handset
1. Alice is on a call.		
2. Alice shouts across the room, "Bob, can you join my call on line 3?"		
3. Bob presses CALLS to display the Call List, and presses ▼ to select the call on line 3.		
4. Bob presses BARGE to barge in the call.		
Bob is now in a conference call with Alice and the caller on line 3.		

Example - picking up a held shared call:

	Alice's handset	Bob's handset
1. Alice is on a call.		
2. Alice presses HOLD to put the call on hold.		
3. Alice shouts across the room, "Bob, can you pick up line 2?"		
4. Bob presses CALLS to display the Call List, and presses ▼ to select the call on line 2.		
5. Bob presses RESUME to pick up the call.		
The call is now on Bob's handset.		

Calls made on an account without assigning to any KeyLine number are considered to be private calls and will not be visible on the Call List of other handsets.

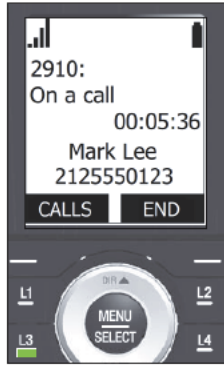
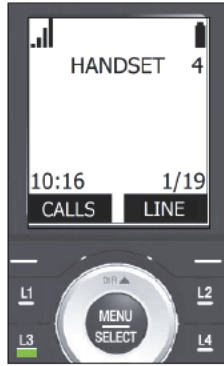
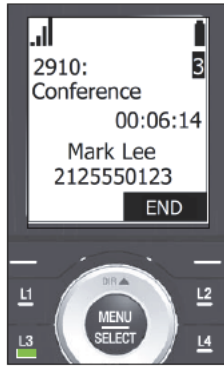
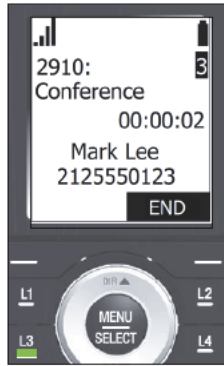
Key System Emulation

Each cordless handset or deskset is equipped with four line keys (L1 to L4) to allow similar usage experience as a typical Key system.



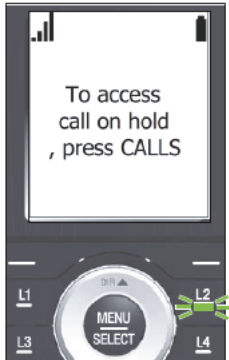



By assigning each Line key to a KeyLine number as done with our factory setting, the user can interact directly with shared calls and perform held call and barge-in conference via pressing the Line key (L1 to L4).

The following scenarios illustrate a Key system experience via direct interactions with the Line keys.

Example - barging in a shared call:

	Alice's handset	Bob's handset
1. Alice is on a call.		
2. Alice shouts across the room, "Bob, can you join my call on line 3?"		
3. Bob presses L3 to barge in the call.		
Bob is now in a conference call with Alice and the caller on line 3.		

Example - picking up a held shared call:

	Alice's handset	Bob's handset
1. Alice is on a call.		
2. Alice presses HOLD to put the call on hold.		
3. Alice shouts across the room, "Bob, can you pick up line 2?"		
4. Bob presses L2 to pick up the call.		
The call is now on Bob's handset.		

CHAPTER 2

CONFIGURATION USING THE PHONE MENUS

The VDP650 Main Menu has the following sub-menus:

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

This chapter contains instructions for using the Admin Settings menu and for accessing the Status menu. See the VDP650/VDP651 User Guide for more information about the other menus.

Viewing the Main Menu

To use the VDP651 menu:

1. When the VDP651 is idle, press **MENU/SELECT**.
The **Main Menu** appears.
2. Press ▼ or ▲ to highlight the desired sub-menu, and then press **MENU/SELECT**.



- Press **SELECT** or an appropriate soft key to save changes.
- Press **OFF/CANCEL** to cancel an operation, exit the menu display or return to the idle screen.

Using the Status menu

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

You can also find the software version of the VDP650 on the **Product Info** screen, available from the **Status** menu.

To view the Status menu:

1. When the VDP651 is idle, press **MENU/SELECT**.
2. On the **Main Menu**, press ▲ or ▼ to highlight **Status**, and then press **MENU/SELECT**.
The **Status** menu appears.
3. On the **Status** menu, press ▲ or ▼ to highlight the desired menu, and then press



MENU/SELECT.

The available status menus are listed in Table 2.

Table 2. Status menu summary

Menu	Information listed
1. Network	<ul style="list-style-type: none"> ■ IP address ■ DHCP status (Enabled/Disabled) ■ Subnet Mask ■ Gateway IP address ■ DNS server 1 IP address ■ DNS server 2 IP address
2. Line	<p>Lines and registration status. On the Line menu, highlight and select the desired line to view detailed line status information:</p> <ul style="list-style-type: none"> ■ Line status (Registered/Not registered) ■ Account display name ■ Account User ID ■ Server IP address
3. Product Info	<p>Shows the product info for the handset or base station. Select Handset or Base to view the:</p> <ul style="list-style-type: none"> ■ Model number (Handset only) ■ Serial number (Handset only) ■ Firmware version ■ V-Series ■ Hardware version

Viewing Line status

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

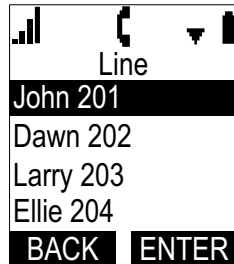
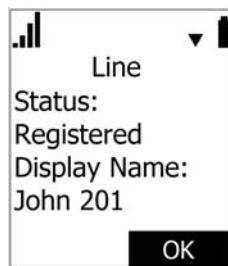


Table 3. Line status icons

Icon	Description
	Line registered
	Line unregistered

To view complete status information for a line:

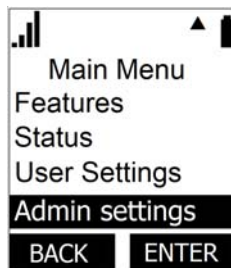
On the **Line** menu, press ▲ or ▼ to highlight the desired line, and then press **MENU/SELECT**. The full line status screen appears.



Using the Admin Settings Menu

To access the Admin Settings menu:

1. When the VDP651 is idle, press **MENU/SELECT**.
The **Main Menu** appears.
2. Press ▲ or ▼ to highlight **Admin settings**, and then press **MENU/SELECT**.



3. Use the dial pad to enter the admin password, and then press **ENTER**. The default password is **admin** (press the * key to enable entering lower-case letters).



The Admin settings are listed in Table 4.

Table 4. Admin setting summary

Setting	Options
Network setting	DHCP (Enable, Disable) Set static IP VLAN ID Others
Security	Secure Browsing
Provisioning	Server string Login ID Login PW
Edit PIN code	Edit PIN
Firmware update	Select Firmware update to have the handset check whether a firmware update is available. See “Updating a Cordless Handset/Deskset” on page 88 .

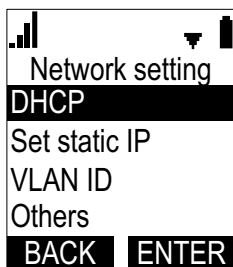
Using the Network Setting menu

Use the Network setting menu to configure network-related settings for the VDP650. For more information about these settings, see [“Basic Network Settings” on page 65](#) and [“Advanced Network Settings” on page 67](#).

To use the Network setting menu:

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

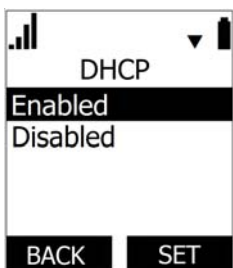
2. Press ▲ or ▼ to highlight the desired option, and then press **MENU/SELECT**:



- DHCP
- Set static IP
- VLAN ID
- Others (DNS and NTP servers).

To enable or disable DHCP:

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



2. Press ▲ or ▼ to select **Enabled** or **Disabled**, and then press **SET**.

DHCP is enabled by default, which means the VDP650 will get its IP address from the network. When DHCP is disabled, you must enter a static IP address for the VDP650.



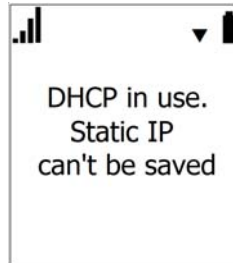
NOTE

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

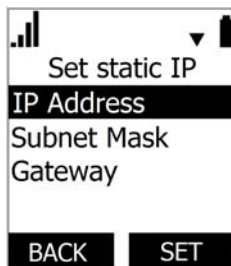
To set static IP for the VDP650:

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

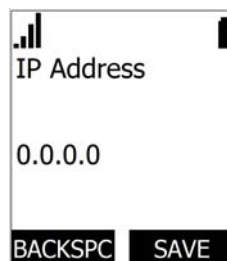
If DHCP is disabled, the **Set static IP** menu appears. If DHCP is enabled, an error message appears briefly before returning you to the **Network setting** menu.



2. On the **Set static IP** menu, with **IP Address** highlighted, press **MENU/SELECT**.



3. Enter the Static IP Address.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.
 - To add a period, press the * key.

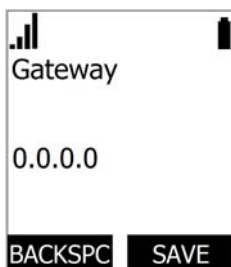


4. Press **SAVE**.
5. On the **Set static IP** menu, press ▲ or ▼ to highlight **Subnet Mask**, and then press **MENU/SELECT**.
6. Enter the Subnet Mask.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.

- To add a period, press the * key.



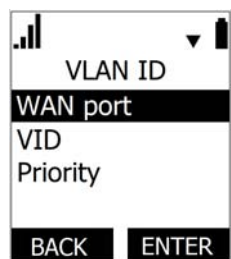
- Press **SAVE**.
- On the **Set static IP** menu, press ▲ or ▼ to highlight **Gateway**, and then press **MENU/SELECT**.
- Enter the Gateway.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.
 - To add a period, press the * key.



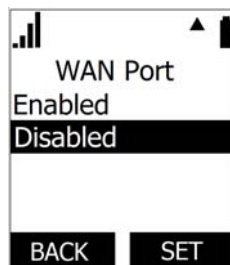
- Press **SAVE**.

To set the VLAN ID for the VDP650:

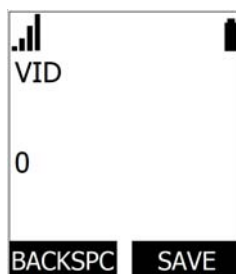
- From the **Network setting** menu, press ▲ or ▼ to highlight **VLAN ID**, and then press **MENU/SELECT**.



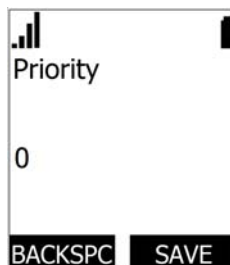
- On the **VLAN ID** menu, with **WAN port** highlighted, press **MENU/SELECT**.



3. Press ▲ or ▼ to select **Enabled** or **Disabled**, and then press **SET**.
4. On the **VLAN ID** menu, press ▲ or ▼ to highlight **VID**, and then press **MENU/SELECT**.
5. Enter the WAN VID. The valid range is 0 to 4095.
 - Use the dial pad to enter numbers.
 - Press **BACKSPC** to delete numbers.



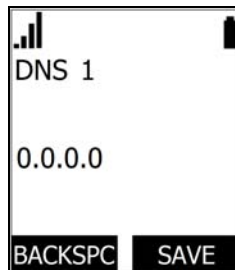
6. Press **SAVE**.
7. On the **VLAN ID** menu, press ▲ or ▼ to highlight **Priority**, and then press **MENU/SELECT**.
8. Enter the WAN Priority. The valid range is 0 to 7.
 - Use the dial pad to enter numbers.
 - Press **BACKSPC** to delete numbers.



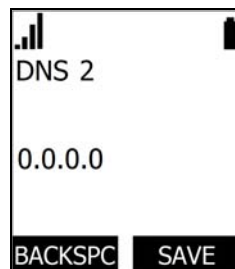
9. Press **SAVE**.

To set other settings (DNS and NTP):

1. From the **Network setting** menu, press ▲ or ▼ to highlight **Others**, and then press **MENU/SELECT**.
2. On the **Others** menu, with **DNS 1** highlighted, press **MENU/SELECT**.
3. Enter the IP address for the primary DNS server.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.



4. Press **SAVE**.
5. On the **Others** menu, press ▲ or ▼ to highlight **DNS 2**, and then press **MENU/SELECT**.
6. Enter the IP address for the secondary DNS server. The VDP650 uses this server if the primary server does not respond.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.



7. Press **SAVE**.
8. On the **Others** menu, press ▲ or ▼ to highlight **NTP**, and then press **MENU/SELECT**.
9. Enter the IP address for the NTP server. If the VDP650 does not use an NTP server, you must manually enter the time and date settings.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.



10. Press **SAVE**.

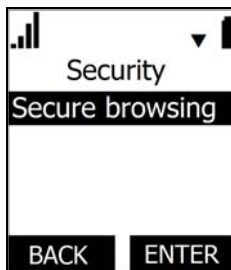
Using the Security menu

Use the Security menu to configure secure browsing settings.

To turn on/off secure browsing:

1. From the **Admin Settings** menu, press ▼ to highlight **Security**, and then press **MENU/SELECT**.

The Security menu appears.



2. With **Secure Browsing** selected, press **ENTER**.
3. Press ▲ or ▼ to select **Enabled** or **Disabled**, and then press **ENTER**.
4. Press **NO** or **YES** on the message “Reboot Base to apply new Web Server settings?”

Using the Provisioning menu

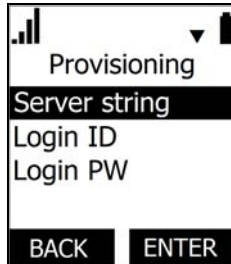
Use the Provisioning menu to configure auto-provisioning settings. For more information about auto-provisioning, see [“Provisioning” on page 91](#) and [“Provisioning Using Configuration Files” on page 106](#).

On the Provisioning menu you can configure:

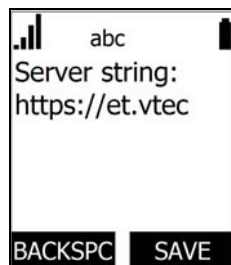
- Server string—the URL of the provisioning server. The URL can include a complete path to the configuration file.
- Login ID—the username the VDP650 will use to access the provisioning server.
- Login PW—the password the VDP650 will use to access the provisioning server.

To use the Provisioning menu:

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



2. On the **Provisioning** menu, with **Server string** highlighted, press **MENU/SELECT**.
3. Enter the URL of the provisioning server.
 - Press **BACKSPC** to delete numbers.
 - Press **1**, **0** and **#** to enter symbols. The period and "@" symbols are available under the **0** key.
 - Use the dial pad to enter numbers.



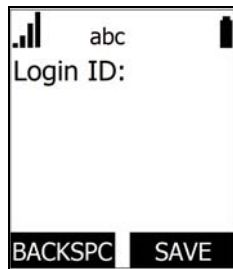
The format of the URL must be RFC 1738 compliant, as follows:

"<schema>://<user>:<password>@<host>:<port>/<url-path>"

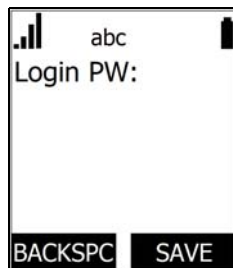
"<user>:<password>@" may be empty.

"<port>" can be omitted if you do not need to specify the port number.

4. Press **SAVE**.
5. On the **Provisioning** menu, press ▲ or ▼ to highlight **Login ID**, and then press **MENU/SELECT**.
6. Enter the Login ID for access to the provisioning server if it is not part of the server string.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.



7. Press **SAVE** .
8. On the **Provisioning** menu, press ▲ or ▼ to highlight **Login PW**, and then press **MENU/SELECT**.
9. Enter the Login password.
 - Press **BACKSPC** to delete numbers.
 - Use the dial pad to enter numbers.



10. Press **SAVE** .

Editing the handset PIN code

To edit the PIN code:

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

The **Enter old PIN** screen appears.



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

CHAPTER 3

USING THE WEBUI

The WebUI allows you to configure all aspects of VDP650 4-Line base station operation, including account settings, network settings, contact lists, and provisioning settings. The WebUI is embedded in the VDP650 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 VDP650 settings. This chapter covers:

- [*“Using the Web User Interface \(WebUI\)” on page 34*](#)
- [*“Status Page” on page 37*](#)
- [*“System Pages” on page 39*](#)
- [*“Network Pages” on page 64*](#)
- [*“Contacts Pages” on page 70*](#)
- [*“Servicing Pages” on page 82.*](#)

Using the Web User Interface (WebUI)

The Web User Interface (WebUI) resides on the VDP650 4-Line base station. You can access it using an Internet browser. After you log in to the WebUI, you can configure the VDP650 on the following pages:

System

- SIP Account Management (see [page 39](#))
- Call Settings (see [page 52](#))
- User Preferences (see [page 54](#))
- Handset Settings (see [page 54](#))
- Server Application (see [page 59](#))

Network

- Basic Network Settings (see [page 65](#))
- Advanced Network Settings (see [page 67](#))

Contacts

- Base Directory (see [page 70](#))
- Blacklist
- LDAP (see [page 77](#))
- Remote XML (see [page 80](#))

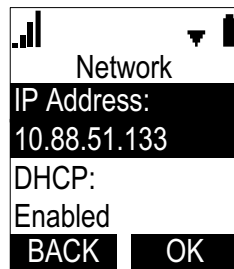
Servicing

- Reboot (see [page 82](#))
- Time and Date (see [page 82](#))
- Firmware Upgrade (see [page 86](#))
- Provisioning (see [page 91](#))
- Security (see [page 97](#))
- Certificates (see [page 101](#))
- Tr069 (see [page 103](#))
- System Logs (see [page 104](#))

The WebUI also has a **System Status** and a **Handset Status** page, where you can view network status and general information about the VDP650 and handsets. The information on the Status page matches the **Status** menu available on the VDP650 handset.

To access the WebUI:

1. Ensure that your computer is connected to the same network as the VDP650.
2. Find the IP address of the VDP650:
 - a. On a handset, press **MENU/SELECT**.
 - b. Press ▼ to highlight **Status**, and then press **MENU/SELECT**.
 - c. With **Network** highlighted, press **MENU/SELECT**.
The **Network** status screen appears.
 - d. On the **Network** status screen, note the IP Address.
3. On your computer, open an Internet browser. (Depending on your browser, some of the



pages presented here may look different and have different controls. Ensure that you are running the latest update of your preferred browser.)

4. Type the VDP650 IP address in the browser address bar and press **ENTER** on your computer keyboard.
The browser displays a window asking for your user name and password.
5. For the user name, enter **admin**. For the password, enter the default password, **admin**. You can change the password later on the WebUI **Security** page, available under **Servicing**.
6. Click **OK**.
The WebUI appears.

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

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

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



The settings tables in this section contain settings that appear in the WebUI and their equivalent settings in the configuration file template. You can use the configuration file template to create custom configuration files. Configuration files can be hosted on a provisioning server and used for automatically configuring phones. For more information, see [“Provisioning Using Configuration Files” on page 106](#).

Status Page

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

System Status

The System Status page shows:

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

STATUS	STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING
System Status	General				
Handset Status	Model: VDP650 Serial Number: 07900002999 MAC Address: 14:AE:DB:2A:40:1D Link Status: Connected Boot Version: 1.13 Software Version: 1.0.0.2 V-Series: 2.10.34.9d38 Hardware Version: HW1.1 EMC Version: 0 Network Time Settings: us.pool.ntp.org				
	Account Status				
	Account 1: Registered Account 2: Not Registered Account 3: Not Registered Account 4: Not Registered Account 5: Not Registered Account 6: Not Registered Account 7: Not Registered Account 8: Not Registered				
	IPv4				
	IP Mode: dhcp IP Address: 10.88.50.107 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: fe80::217:c5ff:fe42:1c7c Primary DNS: Secondary DNS:				

Handset Status

The handset status page shows the name and registration status of cordless handsets. The page lists the maximum of 10 handsets, even if fewer handsets are registered. If you have not given the handsets unique names, the default name of “HANDSET” appears.

STATUS		STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING
System Status		Handset Status				
Handset Status		Handset Status				
		Name		Registration Status		
1:		HANDSET		Not Registered		
2:		HANDSET		Registered		
3:		DESKSET		Registered		
4:		HANDSET		Not Registered		
5:		HANDSET		Not Registered		
6:		HANDSET		Not Registered		
7:		HANDSET		Not Registered		
8:		HANDSET		Not Registered		
9:		HANDSET		Not Registered		
10:		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 116.

SYSTEM	STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING
SYSTEM ACCOUNT MANAGEMENT ACCOUNT 1					
General Account Settings					
<input checked="" type="checkbox"/> Enable Account					
Account label: <input type="text" value="3330"/>					
Display Name: <input type="text" value="3330"/>					
User Identifier: <input type="text" value="3330"/>					
Authentication Name: <input type="text" value="3330"/>					
Authentication Password: <input type="password" value="*****"/>					
Dial Plan: <input type="text" value="x+P"/>					
Inter-Digit Timeout (secs): <input type="text" value="3"/>					
Maximum Number of Calls: <input type="text" value="4"/>					
Feature Synchronization: <input type="text" value="Disable"/>					
DTMF Method: <input type="text" value="Auto"/>					
Unregister After Reboot: <input type="text" value="Disable"/>					
Call Rejection Response Code: <input type="text" value="486"/>					

General Account Settings

Click the link for each setting to see the matching configuration file parameter in [“Configuration File Parameter Guide”](#) on page 114. 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 VDP651 display when account x is selected. The Account Label identifies the SIP account throughout the WebUI and on the handset Dialing Line menu.
Display Name	Enter the Display Name. The Display Name is the text portion of the caller ID that is displayed for outgoing calls using account x.
User identifier	Enter the User identifier supplied by your service provider. The User ID, also known as the Account ID, is a SIP URI field used for SIP registration. Note: Do not enter the host name (e.g. "@sipservice.com"). The WebUI automatically adds the default host name.

Setting	Description
Authentication name	If authentication is enabled on the server, enter the authentication name (or authentication ID) for authentication with the server.
Authentication password	If authentication is enabled on the server, enter the authentication password for authentication with the server.
Dial Plan	Enter the dial plan, with dialing strings separated by a symbol. See “Dial Plan” on page 41 .
Inter Digit Timeout (secs)	Sets how long the VDP651 waits after any "P" (pause) in the dial string or in the dial plan.
Maximum Number of Calls	Select the maximum number of concurrent active calls allowed for that account.
Feature Synchronization	Enables the VDP650 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 VDP651 menu and WebUI. Similarly, changes made using the VDP651 or WebUI will update the settings on the server.
DTMF method	Select the default DTMF transmission method. You may need to adjust this if call quality problems are triggering unwanted DTMF tones or you have problems sending DTMF tones in general.
Unregister after reboot	Enables the phone to unregister the account(s) after rebooting-before the account(s) register again as the phone starts up. If other phones that share the same account(s) unregister unexpectedly in tandem with the rebooting VDP650, disable this setting.
Call Rejection Response Code	<p>Select the response code for call rejection. This code applies to the following call rejection cases:</p> <ul style="list-style-type: none"> ■ 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 VDP651 should dial the number.

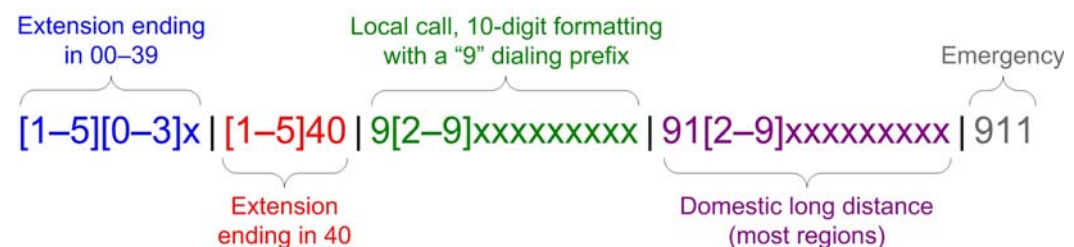


Numbers that are dialed when forwarding a call—when the user manually forwards a call, or a pre-configured number is dialed for Call Forward All, Call Forward–No Answer, or Call Forward Busy—always bypass the dial plan.

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 are 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 39).
(0:9)	This is a substitution rule where the first number is replaced by the second. For example, "(4:723)xxxx" would replace "46789" with "723-6789". If the substituted number (the first number) is empty, the second number is added to the number dialed. For example, in "(:1)xxxxxxxxxx", the digit 1 is appended to any 10-digit number dialed.
	This separator is used to indicate the start of a new pattern. Can be used to add multiple dialing rules to one pattern edit box.

A sample dial plan appears below.



SIP Server Settings

	SIP Server
	Server Address: <input type="text" value="10.88.25.60"/>
	Port: <input type="text" value="5060"/>

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

	Registration
	Server Address: <input type="text" value="10.88.25.60"/>
	Port: <input type="text" value="5060"/>
	Expiration (secs): <input type="text" value="3600"/>
	Registration Freq (secs): <input type="text" value="10"/>

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

	Outbound Proxy
	Server Address: <input type="text"/>
	Port: <input type="text" value="5060"/>

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

	Backup Outbound Proxy	
	Server Address:	<input type="text"/>
	Port:	<input type="text" value="5060"/>

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

	Caller Identity	
	Source Priority 1:	<input type="text" value="PAI"/>
	Source Priority 2:	<input type="text" value="RPID"/>
	Source Priority 3:	<input type="text" value="From"/>

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

	Audio	
	Codec Priority 1:	<input type="text" value="G.722"/>
	Codec Priority 2:	<input type="text" value="G.711u"/>
	Codec Priority 3:	<input type="text" value="None"/>
	Codec Priority 4:	<input type="text" value="None"/>
	Codec Priority 5:	<input type="text" value="None"/>
	Codec priority 6:	<input type="text" value="None"/>
	Codec priority 7:	<input type="text" value="None"/>
	<input type="checkbox"/> Enable Voice Encryption (SRTP)	
	<input type="checkbox"/> Enable G.729 Annex B	
Preferred Packetization Time (ms): <input type="text" value="20"/>		
DTMF Payload Type: <input type="text" value="101"/>		

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.

Setting	Description
Codec priority 4	Select the codec to be used fourth during a call if the previous codec fails.
Codec priority 5	Select the codec to be used fifth during a call if the previous codec fails.
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 seventh 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 (signalling)	Enter the Differentiated Services Code Point (DSCP) value from the Quality of Service setting on your router or switch.

Signaling Settings

Setting	Description
Local SIP port	Enter the local SIP port.
Transport	<p>Select the SIP transport protocol:</p> <ul style="list-style-type: none">■ TCP (Transmission Control Protocol) is the most reliable protocol and includes error checking and delivery validation.■ UDP (User Datagram Protocol) is generally less prone to latency, but SIP data may be subject to network congestion.■ TLS (Transport Layer Security)—the VDP650 supports secured SIP signalling via TLS. Optional server authentication is supported via user-uploaded certificates. TLS certificates are uploaded using the configuration file. See “file” Module: Imported File Settings on page 163 and consult your service provider.

Voice Settings

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 Settings

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

Feature Access Codes	
Voicemail	<input type="text"/>
DND ON:	<input type="text"/>
DND OFF:	<input type="text"/>
Call Forward All ON:	<input type="text"/>
Call Forward All OFF:	<input type="text"/>
Call Forward No Answer ON:	<input type="text"/>
Call Forward No Answer OFF:	<input type="text"/>
Call Forward Busy ON:	<input type="text"/>
Call Forward Busy OFF:	<input type="text"/>
Anonymous Call Reject ON:	<input type="text"/>
Anonymous Call Reject OFF:	<input type="text"/>
Anonymous Call ON	<input type="text"/>
Anonymous Call OFF	<input type="text"/>

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

Setting	Description
Anonymous Call Reject OFF	Enter the Anonymous Call Reject OFF access code.
Anonymous Call ON	Enter the Anonymous Call ON access code.
Anonymous Call OFF	Enter the Anonymous Call OFF access code.

Voicemail Settings

Voicemail Settings	
<input checked="" type="checkbox"/> Enable MWI subscription	
Mailbox ID:	<input type="text"/>
Expiration (secs)	<input type="text" value="3600"/>
<input type="checkbox"/> Ignore Unsolicited MWI:	

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	<p>When selected, unsolicited MWI notifications—notifications in addition to, or instead of SUBSCRIBE and NOTIFY methods—are ignored for account x. If the VDP650 receives unsolicited MWI notifications, the Message Waiting LED will not light to indicate new messages. Disable this setting if:</p> <ul style="list-style-type: none"> ■ 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 VDP650 receives unsolicited MWI notifications.

NAT Traversal

	NAT Traversal	
	<input type="checkbox"/> Enable STUN	
	Server address:	<input type="text"/>
	Port:	<input type="text" value="3478"/>
	<input checked="" type="checkbox"/> Enable UDP Keep-Alive	
	Keep-alive interval (secs):	<input type="text" value="30"/>

Setting	Description
Enable STUN	Enables or disables STUN (Simple Traversal of UDP through NATs) for account x. The Enable STUN setting allows the VDP650 to identify its publicly addressable information behind a NAT via communicating with a STUN server.
Server address	Enter the STUN server IP address or domain name.
Server port	Enter the STUN server port.
Enable UDP Keep-Alive	Enables or disables UDP keep-alives. Keep-alive packets are used to maintain connections established through NAT.
Keep-alive interval (secs)	Enter the interval (in seconds) for sending UDP keep-alives.

Music on Hold Settings

	Music On Hold	
	<input type="checkbox"/> Enable Local MoH	

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

	Network Conference	
	<input type="checkbox"/> Enable Network Conference	
	Conference URI:	<input type="text"/>

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

Session Timer
☐ Enable Session Timer
Minimum value (secs):
Maximum value (secs):

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

Jitter Buffer
☐ Fixed
Fixed Delay (ms):
☒ Adaptive
Normal Delay (ms):
Minimum Delay (ms):
Maximum Delay (ms):

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

Keep Alive
☐ Enable Keep Alive
Keep Alive interval (secs):
☒ Ignore Keep Alive Failure

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 159.

General Call Settings

SYSTEM
SIP Account Management
Account 1
Account 2
Account 3
Account 4
Account 5
Account 6
Call Settings
Account 1
Account 2
Account 3
Account 4
Account 5
Account 6
User Preferences
Signaling
Handset Settings
Account Assignments
Handset Name

STATUSSYSTEMNETWORKCONTACTSSERVICING

SYSTEM CALL SETTINGS 1

General Call Settings

☐ Anonymous Call Reject
☐ Enable Anonymous Call

Do Not Disturb

☐ Enable DND

Call Forward

☐ Enable Call Forward Always
Target number:
☐ Enable Call Forward Busy
Target number:
☐ Enable Call Forward No Answer
Target number:
Delay:

Save

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

Do Not Disturb

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

Call Forward

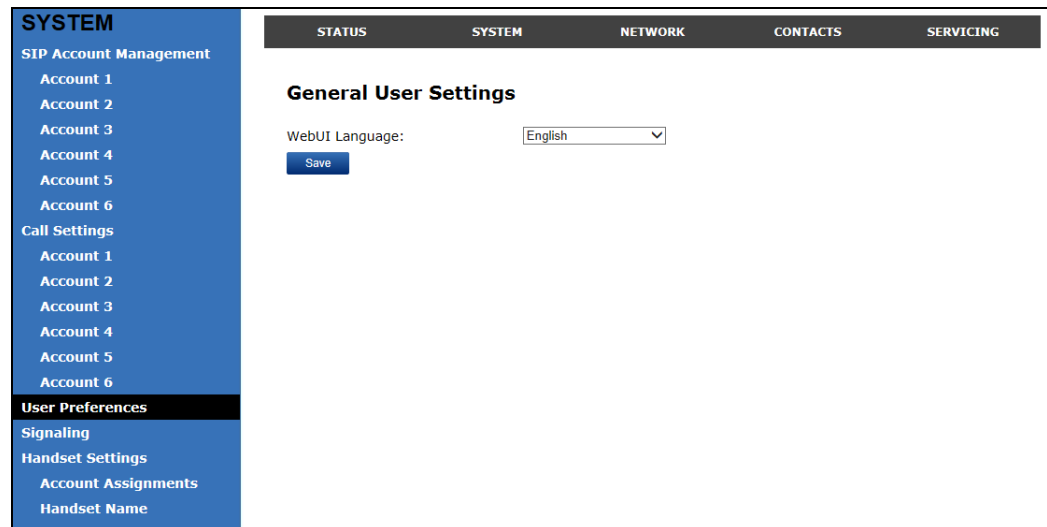
Setting	Description
Enable Call Forward Always	Enables or disables call forwarding for all calls on that line. Select to enable.
Target Number	Enter a number to which all calls will be forwarded.

Setting	Description
Enable Call Forward Busy	Enables or disables forwarding incoming calls to the target number if: <ul style="list-style-type: none">■ 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.

User Preferences

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

The preference settings are also available as parameters in the configuration file. See [“user_pref” Module: User Preference Settings](#) on page 158.



The screenshot shows the VDP650 WebUI interface. On the left, a blue sidebar contains the 'SYSTEM' menu with options like 'SIP Account Management', 'Account 1' through 'Account 6', 'Call Settings', 'User Preferences' (highlighted), 'Signaling', 'Handset Settings', 'Account Assignments', and 'Handset Name'. The main content area has a dark header with tabs: 'STATUS', 'SYSTEM', 'NETWORK', 'CONTACTS', and 'SERVICING'. Below the header, the 'General User Settings' section is visible, featuring a 'WebUI Language' dropdown menu currently set to 'English' and a 'Save' button.

General User Settings

Click the link for each setting to see the matching configuration file parameter in [“Configuration File Parameter Guide”](#) on page 114. Default values and ranges are listed there.

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

Handset Settings

The Handset Settings allow you to configure account assignments and names for the cordless handsets that are registered to the base station. For more information on registering cordless handsets, see the VDP650/VDP651 User Guide.

The network settings are also available as parameters in the configuration file. See [“hs_settings” Module: Handset Settings](#) on page 128.

Account Assignments

The **Account Assignments** table lists the maximum of 10 handsets, even if there are fewer handsets registered. The registration status of currently registered handsets does not affect what is listed on this table.

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

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

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

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

SYSTEM

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
Handset Settings
Account Assignments
KeyLine Assignments
Repeater Mode
Handset Name

STATUS

SYSTEM

NETWORK

CONTACTS

SERVICING

Account Assignments

	Handset Name	Account 1	Account 2	Account 3	Account 4	Account 5	Account 6	Account 7	Account 8	Default
1	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
2	DESKSET	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
3	HANDSET	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
4	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
5	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
6	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
7	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
8	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
9	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼
10	HANDSET	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account 1 ▼

Save

KeyLine Assignments

On the KeyLine Assignments page, you can assign accounts to KeyLine numbers. KeyLine assignments apply to all handsets and desksets registered to the VDP650 SIP DECT 4-Line base station.

The KeyLine number is displayed on the handset/deskset when you are on a call or displaying calls in the Call List. The KeyLine number identifies the line number of a call.

Because a maximum of four active SIP sessions are supported across all handsets and desksets, you should only configure a maximum of four KeyLine assignments.

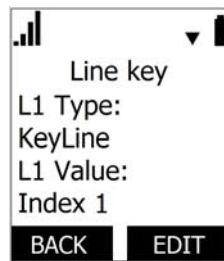
The factory default is set to Account 1 for Keyline 1 to 4.

KeyLine	Account
KeyLine 1:	Account 1
KeyLine 2:	Account 1
KeyLine 3:	Account 1
KeyLine 4:	Account 1
KeyLine 5:	N/A
KeyLine 6:	N/A
KeyLine 7:	N/A
KeyLine 8:	N/A
KeyLine 9:	N/A
KeyLine 10:	N/A
KeyLine 11:	N/A
KeyLine 12:	N/A

Setting	Description
Keyline 1-12	Select the account you want to assign to the corresponding KeyLine number. Default values (1-4): Account 1, (5-12): N/A

To enable a Key System experience for your phone system, you must configure the line keys (L1 to L4) for each handset and deskset. Such configuration is available via the phone user interface (described below), or the configuration file parameters (see ["hs_settings" Module: Handset Settings](#) on page 128).

On the handset/deskset, select **MENU > User Settings > Progrm'able key > Line key**.



For each line key (L1 to L4), assign the KeyLine number that matches the KeyLine numbers you configured in the WebUI KeyLine Assignments.

The factory default configuration to enable a Key System experience is:

L1 Type: KeyLine, L1 Value: Index 1

L2 Type: KeyLine, L2 Value: Index 2

L3 Type: KeyLine, L3 Value: Index 3

L4 Type: KeyLine, L4 Value: Index 4

For more information about configuring the line keys (L1 to L4), see “Configuring the programmable keys” in the VDP650/VDP651 User Guide.

Repeater Mode

On the **Repeater Mode** page, you can enable a repeater (such as the VSP605 Range Extender) to be registered to the base station.

SYSTEM
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
Handset Settings
Account Assignments
KeyLine Assignments
Repeater Mode
Handset Name
Server Application

STATUSSYSTEMNETWORKCONTACTSSERVICING

Repeater Mode

☒ Enable Repeater Mode

Warning: Changing the repeater mode will reboot your device.

Save

Setting	Description
Enable Repeater Mode	Select this check box to enable a repeater to be registered to your VDP650 4-Line base station. Changing this setting requires a reboot of the VDP650 4-Line base station.

Handset Name

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

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

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

STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING
Handset Name				
Handset 1:	<input type="text" value="HANDSET"/>			
Handset 2:	<input type="text" value="DESKSET"/>			
Handset 3:	<input type="text" value="HANDSET"/>			
Handset 4:	<input type="text" value="HANDSET"/>			
Handset 5:	<input type="text" value="HANDSET"/>			
Handset 6:	<input type="text" value="HANDSET"/>			
Handset 7:	<input type="text" value="HANDSET"/>			
Handset 8:	<input type="text" value="HANDSET"/>			
Handset 9:	<input type="text" value="HANDSET"/>			
Handset 10:	<input type="text" value="HANDSET"/>			
Save				

Server Application

On the Server Application page, you can enter Action URIs to allow the VDP650 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 customised to deliver an appropriate user experience.

The VDP650 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 initialised at the beginning and at the end of the call.

Variable value	Description
SIPUSERNAME	SIP Account User Identifier
DISPLAYNAME	SIP Account Display Name
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: <ul style="list-style-type: none"> ■ REGISTERED ■ DEREGISTERED ■ FAIL
MAC	The phone's MAC Address
MODEL	The phone's model number: VDP650.

SYSTEM	STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING
SYSTEM 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 Handset Settings Account Assignments KeyLine Assignments Repeater Mode Handset Name Server Application	Server Application Action URI End of boot sequence: <input type="text"/> Successful Registration: <input type="text"/> On Hook: <input type="text"/> Off Hook: <input type="text"/> Incoming Call: <input type="text"/> Outgoing Call: <input type="text"/> Timer Based: <input type="text"/> Timer Based Interval: <input type="text" value="3600"/> Connected: <input type="text"/> Registration Event: <input type="text"/> XML Push Settings <input type="checkbox"/> Enable HTTP Push: <input type="checkbox"/> Enable Push during call <input type="button" value="Save"/>				

Action URI

Setting	Description
End of boot sequence	<p>The End of boot sequence URI is triggered at the end of the phone boot sequence.</p> <p>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.</p>
Successful Registration	<p>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.</p>
On Hook	<p>The On Hook URI is triggered when the phone transitions from Active to Idle (or from Paging to Idle). For example, when:</p> <ul style="list-style-type: none"> ■ The user presses the End soft key ■ The user hangs up the 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.

Setting	Description
Off Hook	<p>The Off Hook URI is triggered when the user goes to Dial mode by:</p> <ul style="list-style-type: none"> ■ Lifting the handset ■ Pressing the SPEAKER hard key ■ Pressing the [New] soft key during a held call. <p>Note that the Off Hook URI will NOT be triggered when calling a pre-defined number and going immediately to Dialling mode—this event triggers the Outgoing Call URI instead.</p>
Incoming Call	<p>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.</p> <p>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).</p>
Outgoing Call	<p>The Outgoing Call URI is triggered each time a SIP INVITE message is sent (Dialling mode). For example, after:</p> <ul style="list-style-type: none"> ■ Pressing the Dial key in Pre-Dial with populated number ■ Using the dial pad to speed dial a call ■ Dialling a Directory number by going off-hook.
Timer Based	<p>The Timer Based URI will be triggered when the configured timeout expires. The timer starts at the end of the phone boot sequence.</p>
Timer Based Interval	<p>Enter the interval before the Timer Based URI is triggered.</p>
Connected	<p>The Connected URI is triggered each time the phone is in an Active Call or is Paging.</p>
Registration Event	<p>The Registration Event URI is triggered every time there is a registration state change. For example:</p> <ul style="list-style-type: none"> ■ Registered ■ Deregistered ■ Fail (Registration timed out, refused, or expired) <p>The Registration Event URI is not triggered when the same event is repeated.</p>

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.

Network Pages

You can set up the VDP650 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 VDP650 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” LED indication on the base station 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 135.

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

Basic Network Settings

NETWORK

Basic

Advanced

STATUS

SYSTEM

NETWORK

CONTACTS

SERVICING

Basic Network Settings

IPv4

☐ Disable
 ☒ DHCP
 ☐ Static IP

IP Address:

Subnet Mask:

Gateway:

0.0.0.0

0.0.0.0

☐ PPPoE

Username:

Password:

☐ Manually Configure DNS

Primary DNS:

Secondary DNS:

0.0.0.0

0.0.0.0

IPv6

☒ Disable
 ☐ Auto Configuration
 ☐ Static IP

IP Address:

Prefix (0-128):

Gateway:

64

☐ Manually Configure DNS

Primary DNS:

Secondary DNS:

Save



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 135. 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 VDP650 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 VDP650, 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 VDP650, 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 VDP650.
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 VDP650 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 VDP650, 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 VDP650, 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 VDP650.
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

NETWORK

Basic

Advanced

STATUS

SYSTEM

NETWORK

CONTACTS

SERVICING

VLAN

☐ Enable LAN Port VLAN

VID:

Priority:

LLDP-MED

☒ Enable LLDP-MED

Packet Interval (secs):

802.1x

☐ Enable 802.1x

Identity:

MDS Password:

VPN

☐ VPN Enable

VPN Config (file upload):

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 135. Default values and ranges are listed there.

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

LLDP-MED

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

802.1x

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

VPN

You can operate the VDP650 SIP DECT 4-Line base station 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. please contact your dealer.



NOTE




Ensure that NTP or manual time is configured correctly so that the VDP650 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

Base Directory

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

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



Each handset also has its own directory. You can add entries to the handset directory using the handset. For more information, see the VDP650/VDP651 User Guide.

CONTACTS

Base Directory

Blacklist

LDAP

Remote XML

STATUS

SYSTEM

NETWORK

CONTACTS

SERVICING

Base Directory

Select All ☐ [Sort By Last Name](#)

Total: 21	First Name	Last Name	Ringer Tone	Work	Mobile	Other	Account	
<input type="checkbox"/>	Angela	Martin	0	7325550118			1	Edit
<input type="checkbox"/>	Bronwyn	McDonald	0	2325550140			1	Edit
<input type="checkbox"/>	Charlie	Johnson	0	5550198			1	Edit
<input type="checkbox"/>	Dale	Appleton	0		6045550135		1	Edit
<input type="checkbox"/>	David	Carter	3	2325550194	2325550177		2	Edit
<input type="checkbox"/>	Davis	Swerdlow	0		2325550172		1	Edit
<input type="checkbox"/>	Elkhart	Taxi	0		6045550155		1	Edit
<input type="checkbox"/>	Graham	Ball	0		2325550176		1	Edit
<input type="checkbox"/>	Kathryn	Dolphy	0		6045550195		1	Edit
<input type="checkbox"/>	Linda	Miller	0		6045550117		2	Edit
<input type="checkbox"/>	Lydia	Braithwaite	0	2325550157			1	Edit
<input type="checkbox"/>	Martin	Meyers	0	2325550122			1	Edit
<input type="checkbox"/>	Mary	Williams	0		6045550145	6045550146	1	Edit
<input type="checkbox"/>	Richard	Serling	0		6045550141	7875550181	2	Edit
<input type="checkbox"/>	Robert	Brown	2		6045550105		2	Edit
<input type="checkbox"/>	Sandro	Voss	0	2325550149			1	Edit
<input type="checkbox"/>	Stefan	Wheeler	0		2325550161		1	Edit
<input type="checkbox"/>	Susan	Ballance	0		6045550170		1	Edit
<input type="checkbox"/>	Terry	Ng	0		2325550187		1	Edit
<input type="checkbox"/>	Ursula	Baldwin	0	6045550166			1	Edit

[First](#) 1 [Last](#) [Next](#)

[Delete Selected Entries](#)
[Add New Entry](#)
[Clear Directory](#)

Import Base Directory

[Choose File](#)

☐ First line is header, skip

Export Base Directory

[Export XML](#)
[Export CSV](#)

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

Table 5. Base Directory commands

Click	To...
Sort By Last Name	Sort the list by last name.
Edit	Edit information for an entry
Next	View the next page of entries.

Table 5. Base Directory commands

Click	To...
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 XML Export CSV	Export the directory.

To add a new directory entry:

- Click [Add New Entry](#) .
The **Create Base Directory Entry** page appears.

CONTACTS
Base Directory
Blacklist
LDAP
Remote XML

STATUSSYSTEMNETWORKCONTACTSSERVICING

Create Base Directory Entry

First Name:

Last Name:

Ringer Tone:

Account:

Work Number:

Mobile Number:

Other Number:

[Save](#)

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


Create Base Directory Entry

Setting	Description	Range	Default
First Name	Enter the appropriate names in these fields. The maximum length of the first name and last name fields is 15 characters.	n/a	Blank
Last Name			
Ringer Tone	Sets a unique ringer tone for calls from this directory entry.	Auto, Tone 1–10	Tone 1
Account	Sets the account used when you dial this directory entry.	Default Account, Account 1–8	Default Account

Setting	Description	Range	Default
Work Number	Enter the appropriate names and numbers in these fields.	n/a	Blank
Mobile Number			
Other Number			

Directory Import/Export

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

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

**NOTE**




Using the configuration file, you can set whether an imported directory file adds to existing entries or replaces existing entries. See ["file" Module: Imported File Settings](#) on page 163.

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

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

Blacklist

On the Blacklist page, you can manage local blacklist entries. The VDP650 rejects calls from numbers that match blacklist entries. You can sort, edit, delete, and add up to 200 blacklist entries. In order to back up your blacklist entries or import another local blacklist file, the page also enables you to export and import the blacklist.

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



You can also use the VDP651 menu to manage blacklist entries. For more information, see the VDP650/VDP651 User Guide.

CONTACTS
Base Directory
Blacklist
LDAP
Remote XML

STATUS
SYSTEM
NETWORK
CONTACTS
SERVICING

Blacklist

Select All ☐ [Sort By Last Name](#)

Total: 3	First Name	Last Name	Home	Work	Mobile	Account	
<input type="checkbox"/>	Aa-Won	Marketing		2325550108		1	Edit
<input type="checkbox"/>	Jordan	Tyler	2325551011			1	Edit
<input type="checkbox"/>	Roger	Fredericks		3215550109		1	Edit

First 1 Last

[Delete Selected Entries](#)
[Add New Entry](#)
[Clear Blacklist](#)

Import Blacklist

[Choose File](#)

☐ First line is header, skip

Export Blacklist

[Export XML](#)
[Export CSV](#)

Table 6 describes the buttons available on the Blacklist page.

Table 6. Blacklist commands

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

Table 6. Blacklist commands

Click	To...
<div>Export XML</div> <div>Export CSV</div>	Export the blacklist.

To add a new blacklist entry:

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

CONTACTS
Base Directory
Blacklist

STATUSSYSTEMNETWORKCONTACTSSERVICING

Create Blacklist Entry

First Name:
Last Name:
Account: ▼
Home Number:
Work Number:
Mobile Number:

Save


- 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 VDP650. After exporting the file, open it in an .xml editor and add or modify entries.

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



Using the configuration file, you can set whether an imported blacklist file adds to or replaces existing entries. See ["file" Module: Imported File Settings](#) on [page 163](#).


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

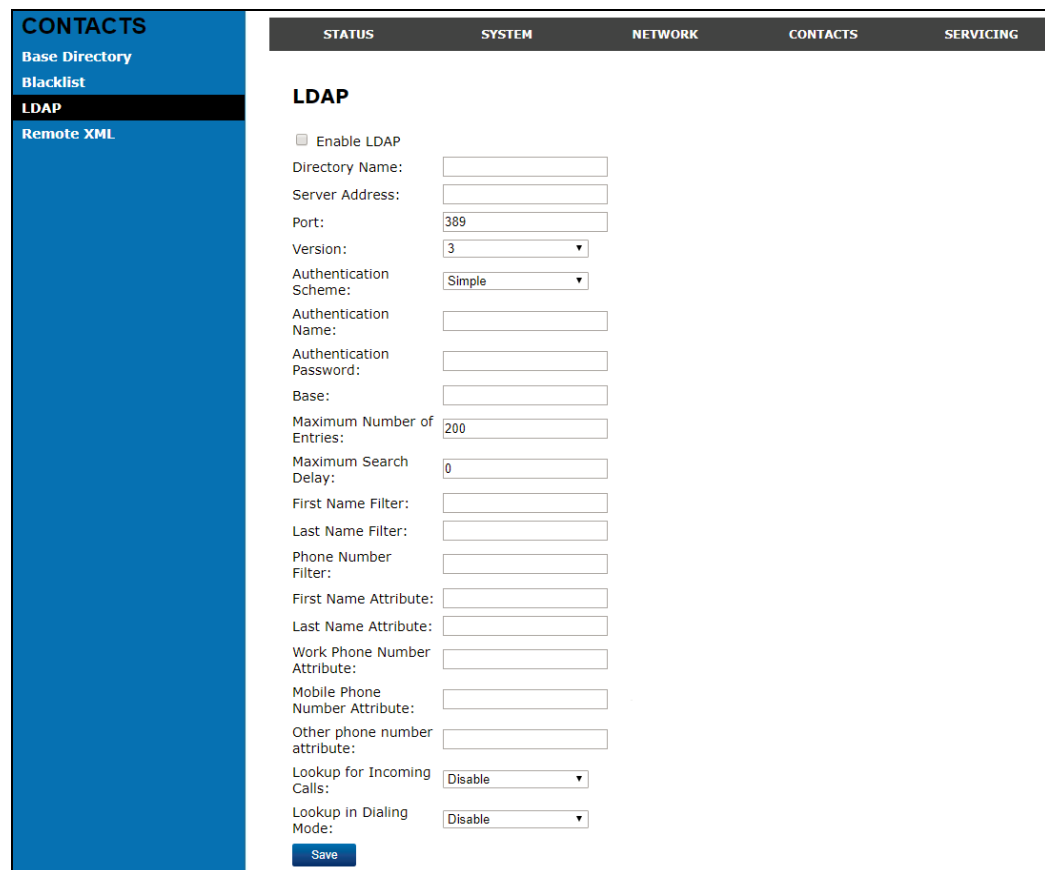
Blacklist WebUI field	Blacklist file XML tag
First Name	<BLACKLIST_ENTRY_NAME_FIRST>
Last Name	<BLACKLIST_ENTRY_NAME_LAST>
Work Number	<BLACKLIST_ENTRY_NUMBER_WORK>
Mobile Number	<BLACKLIST_ENTRY_NUMBER_MOBILE>
Other Number	<BLACKLIST_ENTRY_NUMBER_OTHER>
Account	<BLACKLIST_ENTRY_LINE_NUMBER>

LDAP

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

The LDAP settings are also available as parameters in the configuration file. See [“remoteDir” Module: Remote Directory Settings](#) on page 150.

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



CONTACTS

- Base Directory
- Blacklist
- LDAP**
- Remote XML

LDAP

☐ Enable LDAP

Directory Name:

Server Address:

Port:

Version:

Authentication Scheme:

Authentication Name:

Authentication Password:

Base:

Maximum Number of Entries:

Maximum Search Delay:

First Name Filter:

Last Name Filter:

Phone Number Filter:

First Name Attribute:

Last Name Attribute:


Work Phone Number Attribute:

Mobile Phone Number Attribute:

Other phone number attribute:

Lookup for Incoming Calls:

Lookup in Dialing Mode:



LDAP Settings

Click the link for each setting to see the matching configuration file parameter in [“remoteDir” Module: Remote Directory Settings](#) on page 150. Default values and ranges are listed there.

Setting	Description
Enable LDAP	Enables or disables the phone's access to the LDAP directory.

Setting	Description
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, separated by commas (no spaces). Your directory may include attributes like "cn" (common name) or "ou" (organizational unit) or "dc" (domain component). For example: ou=accounting,dc=vtech,dc=com
Maximum number of entries	Sets the maximum number of entries returned for an LDAP search. Limiting the number of hits can conserve network bandwidth.
Maximum search delay	Enter the delay (in seconds) before the phone starts returning search results.
First name filter	Enter the first name attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
Last name filter	Enter the last name attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
Phone number filter	Enter the number attributes for LDAP searching. The format of the search filter is compliant to the standard string representations of LDAP search filters (RFC 2254).
First name attribute	Sets the attribute for first name. What you enter here should match the first name attribute for entries on the LDAP server (gn for givenName, for example). This helps ensure that the phone displays LDAP entries in the same format as the Local Directory.

Setting	Description
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.

Remote XML

The VDP650 supports three server-hosted Remote XML directories. A total of 5,000 Remote XML directory entries are supported. The 5,000 entries can be shared across the three remote XML directories.

When the user selects a remote directory to view, the VDP650 will sync with the directory server. The handset 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>
```

CONTACTS				
Base Directory				
Blacklist				
LDAP				
Remote XML				
Remote XML Directories				
ID	Name	Remote XML URI	Enable Incoming/Outgoing Call Lookup	
1	Remote1	http://10.88.50.1/xml/1000dir	<input checked="" type="checkbox"/>	
2	Remote2	http://10.88.50.1/xml/xmldir2	<input checked="" type="checkbox"/>	
3			<input type="checkbox"/>	
Save				

Setting	Description
Name	<p>Sets the name of the directory as it will appear on the VDP650 Directory list.</p> <p>The following order applies to the Directory list when multiple server-based directories are enabled:</p> <ol style="list-style-type: none">1. Local2. Blacklist3. LDAP4. Remote XML directory 15. Remote XML directory 26. Remote XML directory 3 <p>Any Remote XML directories will move up the list if LDAP directories are not enabled.</p>
Remote XML URI	<p>Enter the location of the XML directory file, from which the phone will sync and retrieve directory entries.</p>
Enable Incoming/ Outgoing Call Lookup	<p>Enables/disables the call lookup feature for incoming and outgoing calls.</p>

Servicing Pages

Reboot

To manually reboot the VDP650 and apply settings that you have updated, click [Reboot](#).

SERVICING	STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING
Reboot Time and Date Firmware Upgrade Auto Upgrade Manual Upgrade Provisioning Security Certificates Device Certificate Server Certificate System Logs	Reboot Reboot Device: 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 145.

SERVICING	STATUS	SYSTEM	NETWORK	CONTACTS	SERVICING
Reboot Time and Date Custom Language Firmware Upgrade Auto Upgrade Manual Upgrade Provisioning Security Certificates Device Trusted Certificates Tr069 System Logs	Time and Date Format Date Format: <input type="text" value="DD/MM/YY"/> Time Format: <input type="text" value="24 Hour"/> Network Time Settings: <input checked="" type="checkbox"/> Enable Network Time NTP Server: <input type="text" value="us.pool.ntp.org"/> <input type="checkbox"/> Use DHCP (Option 42) Time Zone and Daylight Savings Settings Time Zone: <input type="text" value="-8 United States-Pacif"/> <input checked="" type="checkbox"/> Automatically adjust clock for Daylight Savings <input type="checkbox"/> User-defined Daylight Savings Time Daylight Savings Start: <input type="text" value="March"/> <input type="text" value="Week 2"/> <input type="text" value="Sunday"/> <input type="text" value="02:00"/> Daylight Savings End: <input type="text" value="November"/> <input type="text" value="Week 1"/> <input type="text" value="Sunday"/> <input type="text" value="02:00"/> Daylight Savings Offset (minutes): <input type="text" value="60"/> <input type="checkbox"/> Use DHCP (Option 2/100/101) Manual Time Settings Date: <input type="text" value="17/04/2018"/> Time: <input type="text" value="17:14:11"/> Apply Now Save				

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 145. 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: <ol style="list-style-type: none"> 1. Option 42 2. NTP Server 3. Manual time.

Time Zone and Daylight Savings Settings


Setting	Description
Time Zone	Select your time zone from the list.
Automatically adjust clock for Daylight Savings	Select to adjust the clock for daylight savings time according to the NTP server and time zone setting. To disable daylight savings adjustment, disable both this setting and User-defined Daylight Savings Time.
User-defined DST	Select to set your own start and end dates and offset for Daylight Savings Time. To disable daylight savings adjustment, disable both this setting and Automatically adjust clock for Daylight Savings.
DST Start: Month DST Start: Week DST Start: Day DST Start: Hour	If User-defined DST is enabled, set the start date and time for daylight savings: Month, week, day, and hour.

Setting	Description
DST End: Month DST End: Week DST End: Day DST End: Hour	If User-defined DST is enabled, set the end date and time for daylight savings: Month, week, day, and hour.
Daylight Savings Offset	If User-defined DST is enabled, this specifies the daylight savings adjustment (in minutes) to be applied when the current time is between Daylight Savings Start and Daylight Savings End.
Use DHCP (Option 2/100/101)	If Enable Network Time is selected, select to use DHCP to determine the time zone offset. Options 2, 100 and 101 determine time zone information.

Manual Time Settings

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

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

Click  to start the VDP650 using the manual time settings.

Custom Language

On the Export Translation page, you can export WebUI 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 WebUI. The custom language adds to the existing languages available with the firmware.

Importing a custom language can only be done using the configuration file. See [“file” Module: Imported File Settings](#) on page 163. For details on creating and formatting a translation file, see the Custom Language document at businessphones.vtech.com.

The screenshot shows the VDP650 WebUI interface. On the left is a blue sidebar menu with the 'SERVICING' section expanded, showing options like Reboot, Time and Date, Custom Language (highlighted), Firmware Upgrade, Auto Upgrade, Manual Upgrade, Provisioning, Security, Certificates, Device, Trusted Certificates, Tr069, and System Logs. The main content area has a dark header with tabs for STATUS, SYSTEM, NETWORK, CONTACTS, and SERVICING. Below the tabs, the 'Export Translation' section contains the text 'Export WebUI Translation to File:', a dropdown menu set to 'English', and an 'Export' button.

The available languages for export are identical to the WebUI Language list described in [“User Preferences”](#) on page 54.

The filename of the exported language file will be:

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

Firmware Upgrade

You can update the VDP650 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 VDP650 firmware.

The firmware upgrade settings are also available as parameters in the configuration file. See [“provisioning” Module: Provisioning Settings](#) on page 140.

Firmware Server Settings

Click the link for each setting to see the matching configuration file parameter in [“provisioning” Module: Provisioning Settings](#) on page 140. Default values and ranges are listed there.

Setting	Description
Base Firmware URL	The URL where the VDP650 Base Station firmware update file resides. This should be a full path, including the filename of the firmware file.
Handset Firmware URL	The URL where the VDP651 Cordless Handset firmware update file resides. This should be a full path, including the filename of the firmware file.
Installed Handset Firmware	The version number of handset firmware currently installed.
Cordless Deskset Firmware URL	The URL where the VDP658 Deskset Accessory firmware update file resides. This should be a full path, including the filename of the firmware file.

Setting	Description
Installed Cordless Deskset Firmware	The version number of deskset firmware currently installed.
Server authentication name	Authentication username for the firmware server.
Server authentication password	Authentication password for the firmware server.

To update the firmware immediately:

■ Click [Update Base Firmware Now](#) , [Install Handset Firmware Now](#) , or [Install Cordless Deskset Firmware Now](#) .



You can also configure the VDP650 to check for firmware updates at regular intervals. See [“Provisioning” on page 91](#).

Manual Firmware Update and Upload

On the Manual Firmware Update Settings page, you can upgrade the VDP650, handset, and cordless deskset 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](#), [Install Handset File](#), or [Install cordless deskset File](#).

After clicking [Update from File](#) the VDP650 will update its firmware and restart.

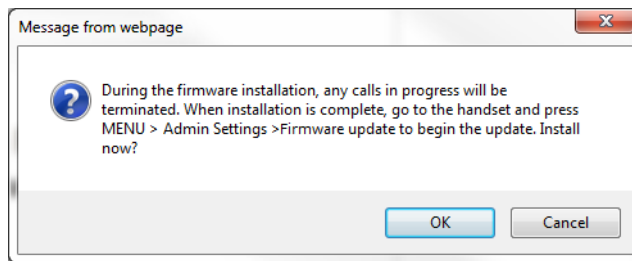
If you are updating handset and/or deskset firmware, you must perform one more procedure after clicking [Install Handset File](#) - see “Updating a Cordless Handset/Deskset”, below.

Updating a Cordless Handset/Deskset

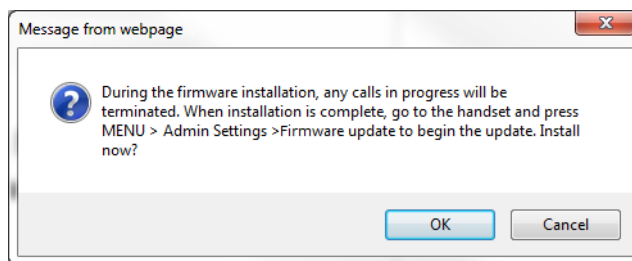
Updating DECT cordless handset/deskset firmware using the WebUI is a two-step process. First you must download the handset/deskset firmware and install it on the base station. Second, you must install the handset/deskset firmware on the handset/deskset. The handset/deskset downloads the firmware over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

To install the handset/deskset firmware on the basestation:

1. **To install the handset firmware:** Click [Install Handset Firmware Now](#) on the **Firmware Server update** page, or [Install Handset File](#) on the **Manual Firmware update** page. The confirmation dialog box shown below appears.



2. **To install the deskset firmware:** Click [Install Cordless Deskset Firmware Now](#) on the **Firmware Server update** page, or [Install cordless deskset File](#) on the **Manual Firmware update** page. The confirmation dialog box shown below appears.



3. To begin installing the handset/deskset 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/deskset.

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

An error message appears if:

- the handset/deskset firmware is already up to date.
- the handset/deskset firmware URL is incorrect, or the file cannot be retrieved for any other reason.
- the handset/deskset firmware file is corrupted.
- the handset/deskset 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/deskset:



Your cordless handset/deskset will automatically initiate the firmware update after a short period of time, as long as there are no active calls on the base station. If you wish to manually start the firmware update, perform the steps below.

1. On the handset/deskset, 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/deskset checks for new firmware. If new firmware is found, the handset/deskset screen asks you to proceed with the update.



NOTE

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

Provisioning

Provisioning refers to the process of acquiring and applying new settings for the VDP650 using configuration files retrieved from a remote computer. After a VDP650 is deployed, subsequent provisioning can update the VDP650 with new settings; for example, if your service provider releases new features. See also [“Provisioning Using Configuration Files” on page 106](#).

With automatic provisioning, you enable the VDP650 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 VDP650 settings (configuration and/or firmware) yourself via **Provisioning > Import Configuration** and/or **Firmware Upgrade > Manual Upgrade**. Manual provisioning can only be performed on one VDP650 at a time.

On the Provisioning page, you can enter settings that will enable the VDP650 to receive automatic configuration and firmware updates. The Provisioning page also allows you to manually update VDP650 configuration from a locally stored configuration file using an Import function. You can also export the VDP650 configuration—either to back it up or apply the configuration to another VDP650 in the future—to a file on your computer.

The provisioning process functions according to the Resynchronization settings and Provisioning Server Settings. The VDP650 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 VDP650 updated to the latest firmware release will have the Redirection Server URL available as the default Provisioning Server URL (see [“provisioning.server_address” on page 144](#)).



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 VDP650 proceeds to the next source until reaching the end of the list.

The provisioning settings are also available as parameters in the configuration file. See [“provisioning” Module: Provisioning Settings” on page 140](#).

SERVICING
Reboot
Time and Date
Firmware Upgrade
Auto Upgrade
Manual Upgrade
Provisioning
Security
Certificates
Device Certificate
Server Certificate
System Logs

STATUSSYSTEMNETWORKCONTACTSSERVICING

Provisioning Server

Server URL:

Server Authentication Name:

Server Authentication Password:

Plug-and-Play Settings

☒ Enable PnP Subscribe

DHCP Settings

☒ Use DHCP Options

DHCP Option Priority 1:

DHCP Option Priority 2:

DHCP Option Priority 3:

Vendor Class ID (DHCP 60):

User Class Info (DHCP 77):

Provisioning Server

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

Plug-and-Play Settings

Setting	Description
Enable PnP Subscribe	Select to enable the VDP650 to search for the provisioning URL via a SUBSCRIBE message to a multicast address (224.0.1.75). The VDP650 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 VDP650 to use DHCP options to locate and retrieve the configuration file. When selected, the VDP650 automatically attempts to get a provisioning server address, and then the configuration file. If DHCP options do not locate a configuration file, then the server provisioning string is checked. Note: Ensure that DHCP is also enabled on the “Basic Network Settings” page.
DHCP Option Priority 1	If DHCP is enabled, sets the DHCP Option priority. Select the highest priority option.
DHCP Option Priority 2	If DHCP is enabled, sets the DHCP Option priority. Select the second highest priority option.
DHCP Option Priority 3	If DHCP is enabled, sets the DHCP Option priority. Select the third highest priority option.
Vendor Class ID (DHCP 60)	DHCP Option 60 is available to send vendor-specific information to the DHCP Server.
User Class Info (DHCP 77)	DHCP Option 77 is available to send vendor-specific information to the DHCP Server.

Resynchronization

On the Resynchronization page, you can select how and when the phone checks for updated firmware and/or configuration files.

Resynchronization

Mode:

Bootup Check:

Schedule Check:

☒ Disable

☐ Interval(minutes)

☐ Days of the Week

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

Start Hour:

End Hour:

☐ Use encryption for configuration file

Passphrase:

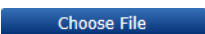

Setting	Description
Mode	Sets which files for which the VDP650 checks. It can check for configuration files, firmware update files (from the URL entered on the Firmware Server Settings page), or both. Note: When checking for both configuration and firmware files, the firmware URL can be within the config file. This firmware URL takes 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 VDP650 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 VDP650 checks for updates.
Start Hour	Select the hour of the day on which the VDP650 checks for updates.
End Hour	Select the hour of the day on which the VDP650 stops checking for updates.
Use encryption	Enables an AES-encrypted configuration file to be decrypted before being applied to the VDP650. Select if the configuration file has been secured using AES encryption. See “Securing configuration files with AES encryption” on page 112 .
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 112 .

Import Configuration

You can configure the VDP650 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 106](#).



To import a configuration file:

1. Click  to locate and open the configuration file.
2. Click  .

The VDP650 will update its configuration.

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

- The VDP650 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 VDP650 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 the following passwords in plain text:

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

Please ensure that you save the exported configuration file in a secure location. You can also disable passwords from being exported as plain text. See [“provisioning.pwd_export_enable” on page 143](#)

To export the configuration file:

- Click  .

The format of the exported file is **<model name>_<mac address>.cfg**. For example, **VDP650_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:

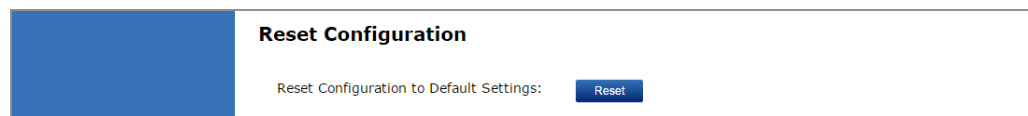
```
#Model Number = xxxxxxxx
```


```
#SW Version = xxxxxxxx
```

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 VDP650 to its default configuration:**

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

Security

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


The security settings are also available as parameters in the configuration file. See [“web” Module: Web Settings” on page 155](#).

Passwords


You can set the administrator password and user password on the WebUI or by using provisioning. For more information on using provisioning to set passwords, see [“profile” Module: Password Settings” on page 172](#).

The screenshot shows the 'SERVICING' section of the WebUI. The left sidebar lists options: Reboot, Time and Date, Firmware Upgrade (Auto Upgrade, Manual Upgrade), Provisioning, Security (highlighted), Certificates (Device Certificate, Server Certificate), and System Logs. The main content area has tabs for STATUS, SYSTEM, NETWORK, CONTACTS, and SERVICING. Under the SERVICING tab, the 'Passwords' section is active. It contains two sub-sections: 'Administrator Password' and 'User Password'. Each sub-section has three input fields: 'Enter Old Password:', 'Enter New Password:', and 'Re-enter New Password:'. A 'Save' button is located at the bottom right of the form.

To change the admin password:

1. Enter the old password (for a new VDP650, 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  .

To change the User password:

1. Enter the old password (for a new VDP650, 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  .

Web Server

Trusted Certificates Tr069 System Logs	Web Server HTTP Server Port: <input type="text" value="80"/> <input checked="" type="checkbox"/> Enable Secure Browsing HTTPS Server Port: <input type="text" value="443"/>
---	---

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 VDP650.

Trusted Servers

The Trusted Servers setting provides a means of blocking unauthorised 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 dialling or other types of server traffic need to be secured), use the Trusted IP settings on the Security page.

<div><div></div><div>Trusted Servers <input type="checkbox"/> Accept SIP account servers only</div></div>	
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.

You 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.



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:

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 authorised IP traffic.

Certificates

You can add two types of certificates using the WebUI or the provisioning file (see [“file” Module: Imported File Settings](#) on page 163). 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 signalling, Provisioning, Firmware, and LDAP directory service. Up to 20 trusted certificates can be installed.

Device Certificate

SERVICING

- Reboot
- Time and Date
- Firmware Upgrade
 - Auto Upgrade
 - Manual Upgrade
- Provisioning
- Security
- Certificates
 - Device Certificate**
 - Server Certificate
 - System Logs

STATUS SYSTEM NETWORK CONTACTS SERVICING

Device Certificate

Custom Certificate:

No file chosen [Choose File](#)

[Import](#)

[Remove Custom 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

SERVICING

- Reboot
- Time and Date
- Custom Language
- Custom Logo
- Firmware Upgrade
 - Auto Upgrade
 - Manual Upgrade
- Provisioning
- Security
- Certificates
- Device
 - Trusted Certificates**
 - Tr069
 - System Logs

STATUS **SYSTEM** **NETWORK** **CONTACTS** **SERVICING**

Trusted Certificate

Select All ☐

Total: 3	Issued to	Issued by	Expiration	Protected
<input type="checkbox"/>	Thawte Premium Server CA	Angela Martin	Jan 1 23:59:59 2021 GMT	<input type="checkbox"/>
<input type="checkbox"/>	Thawte Premium Server CA	John Smith	Jan 1 23:59:59 2021 GMT	<input type="checkbox"/>
<input type="checkbox"/>	Thawte Premium Server CA	Mark Lee	Jan 1 23:59:59 2021 GMT	<input type="checkbox"/>

☐ Only accept trusted certificates

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 . 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).

SERVICING
Reboot
Time and Date
Custom Language
Custom Logo
Firmware Upgrade
Auto Upgrade
Manual Upgrade
Provisioning
Security
Certificates
Device
Trusted Certificates
Tr069
System Logs

STATUSSYSTEMNETWORKCONTACTSSERVICING

TR069

☒ Enable TR069

ACS Username

ACS Password

ACS URL

☐ Enable Periodic Inform

Periodic Inform Interval (seconds)

Connection Request Username

Connection Request Password

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: Log Settings](#) on page 149.

SERVICING

- Reboot
- Time and Date
- Firmware Upgrade
 - Auto Upgrade
 - Manual Upgrade
- Provisioning
- Security
- Certificates
 - Device Certificate
 - Server Certificate
- System Logs**

Syslog

☐ Enable Syslog

Server Address:

Port:

Log Level:

Network Trace

Capture:

Download Log

Save to File:

Syslog Settings




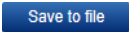
Setting	Description
Enable Syslog	Enable log output to syslog server.
Server address	Syslog server IP address.
Server port	Syslog server port.
Log Level	Sets the log level. The higher the level, the larger the debug output. <ul style="list-style-type: none">■ 5—ALL■ 4—DEBUG■ 3—INFO■ 2—WARNING■ 1—ERROR■ 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 . The button changes to .
2. Stop the network trace by clicking .
3. Save the trace by clicking . Your browser should prompt you to save the **capture.pcap** file.

Download Log

To download the system log:

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

CHAPTER 4

PROVISIONING USING CONFIGURATION FILES

Provisioning using configuration files is the quickest way to configure multiple VDP650 4-Line base stations. You can place configuration files on a provisioning server, where the VDP650 4-Line base stations retrieve the files and update their configuration automatically.

Configuration files have the extension **.cfg** and contain settings that will apply to VDP650 4-Line base stations. To edit a configuration file, open it with a text editor such as Notepad.

The settings within a configuration file are grouped into modules. Most of the modules group their settings in the same way that settings are grouped on the VDP650 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 VDP650 configuration file modules and their associated parameters, see ["Configuration File Parameter Guide" on page 114](#).

Using the WebUI, you can also import a configuration file and apply the configuration file settings to the VDP650. For more information, see ["Import Configuration" on page 95](#).

This chapter covers:

- ["The Provisioning Process" on page 107](#)
- ["Configuration File Types" on page 109](#)
- ["Data Files" on page 110](#)
- ["Configuration File Tips and Security" on page 111](#).

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 91](#) and [“Resynchronization: configuration file checking” on page 108](#). The VDP650 maintains a list of the last loaded provisioning files. The VDP650 compares its current configuration against the files it finds on the provisioning server.

If provisioning has been triggered by the resync timer expiring or by remote check-sync, the VDP650 checks for updated files after one minute of inactivity.

2. Download the configuration files.

If any file on the provisioning server has changed, the VDP650 treats it as a new file and downloads it.

If the provisioning URL specifies a path only with no filename, then by default the VDP650 looks for and retrieves the following two files:

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

The <model> variable is the VTech product model: VDP650, for example.

If the provisioning URL specifies both a path and filename, then the VDP650 retrieves only the configuration file specified.

3. The VDP650 restarts after one minute of inactivity.

During provisioning, the VDP650 reads the configuration file and validates each module and setting. The VDP650 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 114](#) 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 VDP650 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 VDP650 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 VDP650 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).

VDP650 restart

If the VDP650 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 VDP650 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 VDP650 will download the file(s) when there is no call activity.

When you update the VDP650 by importing a configuration file using the WebUI, the device restarts immediately after applying the new settings, regardless of whether the VDP650 is idle.

Configuration File Types

The VDP650 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 VDP650 in the system.

The MAC-specific configuration file is a file that only a single VDP650 can retrieve. The MAC-specific configuration file name contains a VDP650 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, **VDP650**. For more information about the MAC-specific configuration file, see [“Guidelines for the MAC-Specific configuration file” on page 111](#).

If the provisioning URL specifies a path only with no filename, then by default the VDP650 will fetch both files.

However, if the provisioning URL specifies both a path and filename, then the VDP650 will only fetch the single configuration file specified.

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

When the VDP650 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 VDP650 4-Line base stations in the general file, and then overwrite that setting for just a few VDP650 4-Line base stations using the MAC-specific file.

Data Files

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

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

Links to data files are in the configuration file's "file" module. This is where you enter any URLs to the data files that the VDP650 4-Line base station may require.

None of the data files are exported when you export a configuration file from the VDP650. 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 VDP650 import the new file. For a complete list of data file parameters, see ["file" Module: Imported File Settings](#) on page 163.

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) VDP650 4-Line base stations. Such settings might include call settings, language, and NAT settings. You can then edit those settings in the configuration template and save it as the general configuration file. The remaining settings will make up the MAC-specific configuration file, which you will have to copy and edit for each VDP650.

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)

Guidelines for the MAC-Specific configuration file

The VDP650 downloads the MAC-specific configuration file after the general configuration file. You must create a MAC-specific configuration file for each VDP650 in your system. The file name must contain the VDP650 MAC address, which is printed on a label on the bottom of the device. For example, a VTech VDP650 4-Line base station with the MAC address of 00:11:A0:10:6F:2D would download the **VDP650_0011A0106F2D.cfg** file.

**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 VDP650 4-Line base station. Such settings will include SIP account settings such as display name, user ID, and authentication ID.

Securing configuration files with AES encryption

You can encrypt your configuration files to prevent unauthorized users modifying the configuration files. The VDP650 firmware decrypts files using the AES 256 algorithm. After encrypting a file and placing it on your provisioning server, you can enable the VDP650 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 VDP650. 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.

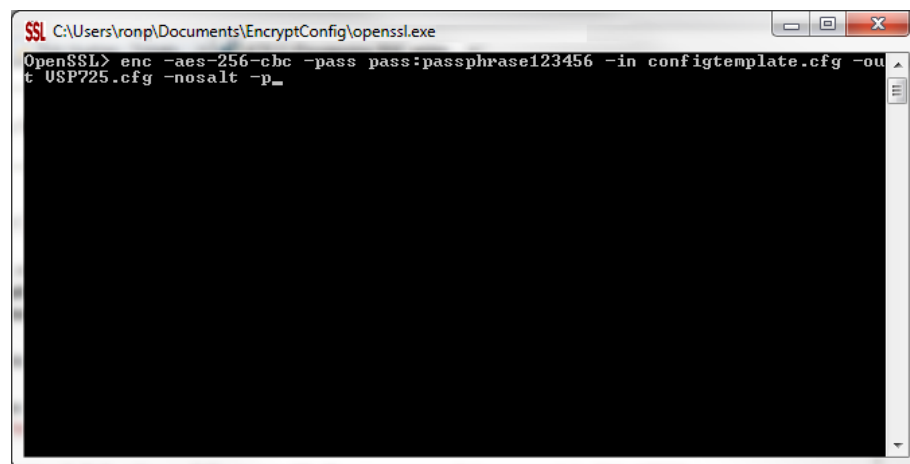


Figure 2. OpenSSL command line

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:
Bootup Check:
Interval:
☒ Use encryption for configuration file
Passphrase

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



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

CHAPTER 5

CONFIGURATION FILE PARAMETER GUIDE

This chapter lists the available options for all the settings within the VDP650 configuration file. Most settings in the configuration file have an equivalent in the WebUI (see the settings tables in [“Using the WebUI” on page 33](#)). 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 VDP650 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 116](#)
- [“hs_settings” Module: Handset Settings” on page 128](#)
- [“network” Module: Network Settings” on page 135](#)
- [“provisioning” Module: Provisioning Settings” on page 140](#)
- [“time_date” Module: Time and Date Settings” on page 145](#)
- [“log” Module: Log Settings” on page 149](#)
- [“remoteDir” Module: Remote Directory Settings” on page 150](#)
- [“web” Module: Web Settings” on page 155](#)
- [“trusted_ip” Module: Trusted IP Settings” on page 156](#)
- [“trusted_servers” Module: Trusted Server Settings” on page 157](#)
- [“user_pref” Module: User Preference Settings” on page 158](#)
- [“call_settings” Module: Call Settings” on page 159](#)

- [*“audio” Module: Audio Settings” on page 161*](#)
- [*“file” Module: Imported File Settings” on page 163*](#)
- [*“tr069” Module: TR-069 Settings” on page 166*](#)
- [*“tone” Module: Tone Definition Settings” on page 168*](#)
- [*“profile” Module: Password Settings” on page 172*](#)

"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 8 for the VDP650.

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 8 for the VDP650.

All these settings are exported when you manually export the configuration from the VDP650.

General configuration file settings

Setting:	sip_account.x.dial_plan		
Description:	Sets the dial plan for account x. See “Dial Plan” on page 41 .		
Values:	Text string	Default:	x+P

Setting:	sip_account.x.call_restrict_dial_plan		
Description:	Enter call restriction dial plan, to prevent users from completing calls to certain numbers for this account.		
Values:	text string (dial plan syntax)	Default:	Blank

Setting:	<code>sip_account.x.inter_digit_timeout</code>		
Description:	Sets the inter-digit timeout (in seconds) for account x. The inter-digit timeout sets how long the VDP650 waits after the last digit is entered before dialing the number.		
Values:	1–10	Default:	3
Setting:	<code>sip_account.x.maximum_call_number</code>		
Description:	Sets the maximum number of concurrent active calls allowed for that account.		
Values:	1–4	Default:	4
Setting:	<code>sip_account.x.dtmf_transport_method</code>		
Description:	Sets the transport method for DTMF signalling for account x.		
Values:	auto, rfc2833, inband, info	Default:	auto
Setting:	<code>sip_account.x.unregister_after_reboot_enable</code>		
Description:	Enables or disables the VDP650 to unregister account x after rebooting.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.primary_sip_server_address</code>		
Description:	Sets the SIP server IP address for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.primary_sip_server_port</code>		
Description:	Sets the SIP server port for account x.		
Values:	1–65535	Default:	5060
Setting:	<code>sip_account.x.primary_registration_server_address</code>		
Description:	Sets the registration server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	Default:	Blank

Setting:	<code>sip_account.x.primary_registration_server_port</code>		
Description:	Sets the registration server port for account x.		
Values:	1–65535	Default:	5060
Setting:	<code>sip_account.x.primary_registration_expires</code>		
Description:	Sets the expiration time (in seconds) of the current registration for account x.		
Values:	30–7200	Default:	3600
Setting:	<code>sip_account.x.registration_retry_time</code>		
Description:	Sets the retry frequency of the current registration for account x.		
Values:	1–1800	Default:	10
Setting:	<code>sip_account.x.primary_outbound_proxy_server_address</code>		
Description:	Sets the outbound proxy server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	Default:	Blank
Setting:	<code>sip_account.x.primary_outbound_proxy_server_port</code>		
Description:	Sets the outbound proxy server port for account x.		
Values:	1–65535	Default:	5060
Setting:	<code>sip_account.x.backup_outbound_proxy_server_address</code>		
Description:	Sets the backup outbound proxy server IP address for account x.		
Values:	IPv4, IPv6 or FQDN	Default:	Blank
Setting:	<code>sip_account.x.backup_outbound_proxy_server_port</code>		
Description:	Sets the backup outbound proxy server port for account x.		
Values:	1–65535	Default:	5060

Setting:	<code>sip_account.x.codec_priority.1</code>
Description:	Sets the highest-priority codec for account x.
Values:	<code>g711u, g711a, g729, g726, g722, g723_1, ilbc</code> Default: <code>g711u</code>
Setting:	<code>sip_account.x.codec_priority.2</code>
Description:	Sets the second highest-priority codec for account x.
Values:	<code>none, g711u, g711a, g729, g726, g722, g723_1, ilbc</code> Default: <code>g711a</code>
Setting:	<code>sip_account.x.codec_priority.3</code>
Description:	Sets the third highest-priority codec for account x.
Values:	<code>none, g711u, g711a, g729, g726, g722, g723_1, ilbc</code> Default: <code>g729</code>
Setting:	<code>sip_account.x.codec_priority.4</code>
Description:	Sets the fourth highest-priority codec for account x.
Values:	<code>none, g711u, g711a, g729, g726, g722, g723_1, ilbc</code> Default: <code>g726</code>
Setting:	<code>sip_account.x.codec_priority.5</code>
Description:	Sets the fifth highest-priority codec for account x.
Values:	<code>none, g711u, g711a, g729, g726, g722, g723_1, ilbc</code> Default: <code>g722</code>
Setting:	<code>sip_account.x.codec_priority.6</code>
Description:	Sets the highest-priority codec for account x.
Values:	<code>g711u, g711a, g729, g726, g722, g723_1, ilbc</code> Default: <code>g723_1</code>
Setting:	<code>sip_account.x.codec_priority.7</code>
Description:	Sets the highest-priority codec for account x.
Values:	<code>g711u, g711a, g729, g726, g722, g723_1, ilbc</code> Default: <code>ilbc</code>

Setting:	<code>sip_account.x.voice_encryption_enable</code>		
Description:	Enables or disables SRTP voice encryption for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.g729_annexb_enable</code>		
Description:	Enables G.729 Annex B, with voice activity detection (VAD) and bandwidth-conserving silence suppression. This setting applies only when G.729a/b is selected in a <code>sip_account.x.codec_priority</code> parameter.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.dscp</code>		
Description:	Sets the Voice Quality of Service Layer 3 - DSCP for account x.		
Values:	0–63	Default:	46
Setting:	<code>sip_account.x.sip_dscp</code>		
Description:	Sets the Signalling Quality of Service Layer 3 - DSCP for account x.		
Values:	0–63	Default:	26
Setting:	<code>sip_account.x.local_sip_port</code>		
Description:	Sets the Local SIP port for account x.		
Values:	1–65535	Default:	Account 1: 5060 Account 2: 5070 Account 3: 5080 Account 4: 5090 Account 5: 5100 Account 6: 5200 Account 7: 5300 Account 8: 5400
Setting:	<code>sip_account.x.transport_mode</code>		
Description:	Sets the Signalling Transport Mode for account x.		
Values:	udp, tcp, tls	Default:	udp

Setting:	<code>sip_account.x.mwi_enable</code>		
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:	<code>sip_account.x.mwi_subscription_expires</code>		
Description:	Sets the MWI subscription expiry time (in seconds) for account x.		
Values:	15–65535	Default:	3600
Setting:	<code>sip_account.x.mwi_ignore_unsolicited</code>		
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:	<code>sip_account.x.nat_traversal_stun_enable</code>		
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:	<code>sip_account.x.nat_traversal_stun_server_address</code>		
Description:	Sets the STUN server IP address.		
Values:	IPv4, IPv6 or FQDN	Default:	Blank
Setting:	<code>sip_account.x.nat_traversal_stun_server_port</code>		
Description:	Sets the STUN server port.		
Values:	1–65535	Default:	3478

Setting:	<code>sip_account.x.nat_traversal_stun_keep_alive_enable</code>		
Description:	Enables or disables UDP keep-alives. Keep-alive packets are used to maintain connections established through NAT.		
Values:	0 (disabled), 1 (enabled)	Default:	1
Setting:	<code>sip_account.x.nat_traversal_stun_keep_alive_interval</code>		
Description:	Sets the interval (in seconds) for sending UDP keep-alives.		
Values:	0-65535	Default:	30
Setting:	<code>sip_account.x.keep_alive_enable</code>		
Description:	Enable SIP keep alive for NAT traversal and monitoring SIP server status.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.keep_alive_interval</code>		
Description:	Sets the interval (in seconds) for sending keep-alives.		
Values:	1-3600	Default:	15
Setting:	<code>sip_account.x.keep_alive_ignore_failure</code>		
Description:	Enable the phone to ignore keep-alive failure, if failure triggers re-subscription (and calls are dropped).		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.music_on_hold_enable</code>		
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:	<code>sip_account.x.sip_session_timer_enable</code>		
Description:	Enables or disables the SIP session timer.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>sip_account.x.sip_session_timer_min</code>		
Description:	Sets the session timer minimum value (in seconds) for account x.		
Values:	90–65535	Default:	90
Setting:	<code>sip_account.x.sip_session_timer_max</code>		
Description:	Sets the session timer maximum value (in seconds) for account x.		
Values:	90–65535	Default:	1800
Setting:	<code>sip_account.x.check_trusted_certificate</code>		
Description:	Enables or disables accepting only a trusted TLS certificate for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.preferred_ptime</code>		
Description:	Enter the packetization interval time in milliseconds.		
Values:	10, 20, 30, 40, 50, 60	Default:	20
Setting:	<code>sip_account.x.cid_src_priority.1</code>		
Description:	Sets the first priority of the caller ID source to be displayed on the incoming call screen.		
Values:	from, pai, rpid	Default:	pai
Setting:	<code>sip_account.x.cid_src_priority.2</code>		
Description:	Sets the second priority of the caller ID source to be displayed on the incoming call screen.		
Values:	none, from, pai, rpid	Default:	rpid
Setting:	<code>sip_account.x.cid_src_priority.3</code>		
Description:	Sets the third priority of the caller ID source to be displayed on the incoming call screen.		
Values:	none, from, pai, rpid	Default:	from

Setting:	<code>sip_account.x.call_rejection_response_code</code>		
Description:	Select the response code for call rejection. This code applies to the following call rejection cases: <ul style="list-style-type: none">■ User presses Reject for an incoming call■ DND is enabled■ Phone rejects a second incoming call with Call Waiting disabled■ Phone rejects an anonymous call with Anonymous Call Rejection enabled■ Phone rejects call when the maximum number of calls is reached		
Values:	480, 486, 603	Default:	486

Setting:	<code>sip_account.x.dtmf_payload_type</code>		
Description:	Set the configurable RTP payload type for in-call DTMF.		
Values:	96-127	Default:	101

Setting:	<code>sip_account.x.use_register_route_header</code>		
Description:	Use Route header for REGISTER		
Values:	0 (disabled), 1 (enabled)	Default:	1

Setting:	<code>sip_account.x.dns_query_option</code>		
Description:	Select DNS query option for SIP traffic only: 0 (DNS query with A record only) 1 (DNS query with NAPTR/SRV/A) DNS query for all other traffic (e.g. HTTP) should always perform A record only.		
Values:	0, 1	Default:	1

MAC-specific configuration file settings

Setting:	<code>sip_account.x.sip_account_enable</code>		
Description:	Enables account x to be used by the device.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>sip_account.x.label</code>		
Description:	Sets the text that identifies the account on the device LCD. The account label appears on the Dialing Line list, dialing screen, and other call appearance screens.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.display_name</code>		
Description:	Sets the text portion of the caller ID that is displayed for outgoing calls using account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.user_id</code>		
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:	<code>sip_account.x.authentication_name</code>		
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:	<code>sip_account.x.authentication_access_password</code>		
Description:	Sets the authentication password for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.feature_sync_enable</code>		
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:	<code>sip_account.x.access_code_retrieve_voicemail</code>		
Description:	Sets the voicemail retrieval feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_dnd_on</code>		
Description:	Sets the do not disturb (DND) ON feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_dnd_off</code>		
Description:	Sets the do not disturb (DND) OFF feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_cfa_on</code>		
Description:	Sets the Call Forward All ON feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_cfa_off</code>		
Description:	Sets the Call Forward All OFF feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_cfna_on</code>		
Description:	Sets the Call Forward No Answer ON feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_cfna_off</code>		
Description:	Sets the Call Forward No Answer OFF feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_cfb_on</code>		
Description:	Sets the Call Forward Busy ON feature access code for account x.		
Values:	Text string	Default:	Blank

Setting:	<code>sip_account.x.access_code_cfb_off</code>		
Description:	Sets the Call Forward Busy OFF feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_anonymous_call_block_on</code>		
Description:	Sets the Anonymous Call Block ON feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_anonymous_call_block_off</code>		
Description:	Sets the Anonymous Call Block OFF feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_outgoing_call_anonymous_on</code>		
Description:	Sets the Anonymous Outgoing Call ON feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.access_code_outgoing_call_anonymous_off</code>		
Description:	Sets the Anonymous Outgoing Call OFF feature access code for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>sip_account.x.mwi_uri</code>		
Description:	Sets the MWI URI that will be used for MWI subscription. If this setting is left blank, the VDP650 uses the account x user ID for MWI subscription.		
Values:	SIP URI text string	Default:	Blank
Setting:	<code>sip_account.x.network_conference_enable</code>		
Description:	Enables or disables network conferencing for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>sip_account.x.network_bridge_uri</code>		
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 account assignments and names for the cordless handsets that are registered to the base station. For more information on registering cordless handsets, see the VDP650/VDP651 User Guide.

General configuration file settings

Setting:	<code>hs_settings.x.handset_us_pin_code</code>
-----------------	--

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

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

Setting:	<code>hs_settings.keyline.y</code>
-----------------	------------------------------------

Description:	Assigns accounts to KeyLine numbers (where y ranges from 1-12 KeyLine numbers). For more information, see "KeyLine Assignments" on page 56 .
---------------------	---

Values:	0-8	Default:	1 (where y = 1-4) 0 (where y = 5-12)
----------------	-----	-----------------	---

Setting:	<code>hs_settings.x.pfk.line1.feature</code>
-----------------	--

Description:	Assign a feature to the L1 line key.
---------------------	---

Values:	unassigned, keyline, line, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	keyline
----------------	---	-----------------	---------

Setting:	<code>hs_settings.x.pfk.line1.account</code>
-----------------	--

Description:	Assign an Account number to the L1 line key.
---------------------	---

Values:	1-8	Default:	1
----------------	-----	-----------------	---

Setting:	<code>hs_settings.x.pfk.line1.value</code>
-----------------	--

Description:	Assign a KeyLine number to the L1 line key.
---------------------	--

Values:	1-12	Default:	1
----------------	------	-----------------	---

Setting:	<code>hs_settings.x.pfk.line2.feature</code>		
Description:	Assign a feature to the L2 line key.		
Values:	unassigned, keyline, line, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	keyline
Setting:	<code>hs_settings.x.pfk.line2.account</code>		
Description:	Assign an Account number to the L2 line key.		
Values:	1-8	Default:	1
Setting:	<code>hs_settings.x.pfk.line2.value</code>		
Description:	Assign a KeyLine number to the L2 line key.		
Values:	1-12	Default:	2
Setting:	<code>hs_settings.x.pfk.line3.feature</code>		
Description:	Assign a feature to the L3 line key.		
Values:	unassigned, keyline, line, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	keyline
Setting:	<code>hs_settings.x.pfk.line3.account</code>		
Description:	Assign an Account number to the L3 line key.		
Values:	1-8	Default:	1
Setting:	<code>hs_settings.x.pfk.line3.value</code>		
Description:	Assign a KeyLine number to the L3 line key.		
Values:	1-12	Default:	3

Setting:	<code>hs_settings.x.pfk.line4.feature</code>		
Description:	Assign a feature to the L4 line key.		
Values:	unassigned, keyline, line, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	keyline
Setting:	<code>hs_settings.x.pfk.line4.account</code>		
Description:	Assign an Account number to the L4 line key.		
Values:	1-8	Default:	1
Setting:	<code>hs_settings.x.pfk.line4.value</code>		
Description:	Assign a KeyLine number to the L4 line key.		
Values:	1-12	Default:	4
Setting:	<code>hs_settings.x.pfk.hold.feature</code>		
Description:	Assign a feature to the HOLD Hard Key.		
Values:	unassigned, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	unassigned
Setting:	<code>hs_settings.x.pfk.hold.account</code>		
Description:	Assign an Account number to the HOLD hard key.		
Values:	1-8	Default:	1
Setting:	<code>hs_settings.x.pfk.intercom.feature</code>		
Description:	Assign a feature to the INTERCOM hard key.		
Values:	unassigned, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	unassigned

Setting:	<code>hs_settings.x.pfk.intercom.account</code>		
Description:	Assign an Account number to the INTERCOM hard key.		
Values:	1-8	Default:	1
Setting:	<code>hs_settings.x.pfk.mute.feature</code>		
Description:	Assign a feature to the MUTE hard key.		
Values:	unassigned, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	unassigned
Setting:	<code>hs_settings.x.pfk.mute.account</code>		
Description:	Assign an Account number to the MUTE hard key.		
Values:	1-8	Default:	1
Setting:	<code>hs_settings.x.pfk.up.feature</code>		
Description:	Assign a feature to the UP hard key.		
Values:	unassigned, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	VDP651: dir VDP658: unassigned
Setting:	<code>hs_settings.x.pfk.up.account</code>		
Description:	Assign an Account number to the UP hard key.		
Values:	1-8	Default:	1
Setting:	<code>hs_settings.x.pfk.down.feature</code>		
Description:	Assign a feature to the DOWN hard key.		
Values:	unassigned, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	VDP651: call log VDP658: unassigned

Setting:	<code>hs_settings.x.pfk.down.account</code>		
Description:	Assign an Account number to the DOWN hard key.		
Values:	1-8	Default:	1

Setting:	<code>hs_settings.x.pfk.softkeyleft.feature</code>		
Description:	Assign a feature to the LEFT soft key.		
Values:	unassigned, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	unassigned

Setting:	<code>hs_settings.x.pfk.softkeyleft.account</code>		
Description:	Assign a feature to the LEFT soft key.		
Values:	1-8	Default:	1

Setting:	<code>hs_settings.x.pfk.softkeyright.feature</code>		
Description:	Assign a feature to the RIGHT soft key.		
Values:	unassigned, call list, dir, call log, redial, messages, dnd, cfwd all, cfwd busy, cfwd no answer	Default:	unassigned

Setting:	<code>hs_settings.x.pfk.softkeyright.account</code>		
Description:	Assign an Account number to the RIGHT soft key.		
Values:	1-8	Default:	1

MAC-specific configuration file settings

Setting:	<code>hs_settings.x.handset_name</code>		
Description:	Sets the name for handset x. You can use up to 11 letters and/or numbers. Use alphanumeric characters only—no symbol characters are allowed.		
Values:	Text string	Default:	HANDSET

Setting:	<code>hs_settings.x.default_account</code>		
Description:	Sets the default account for handset x. The handset attempts to use this account first when going off hook.		
Values:	1–6	Default:	1

Setting:	<code>hs_settings.x.assigned_account</code>		
Description:	Sets the accounts for handset x that will be available for incoming and outgoing calls. List account numbers separated by commas (for example, 1,2,3,4,5,6,7,8).		
Values:	1–8	Default:	1,2,3,4,5,6,7,8

system Module: System settings

The System settings enables you to configure DECT related settings for the VDP650 4-Line base station.

General configuration file settings

Setting:	<code>system.repeater_mode_enable</code>		
Description:	Enables a repeater (such as the VSP605 Range Extender) to be registered to the VDP650 4-Line base station.		
Values:	0 (disabled), 1 (enabled)	Default:	0

Setting:	<code>system.eco</code>		
Description:	Enables or disables ECO mode.		
Values:	0 (disabled), 1 (enabled)	Default:	0

"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.lldp_med.enable		
-----------------	-------------------------	--	--

Description:	Enables or disables LLDP-MED.		
---------------------	-------------------------------	--	--

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

Setting:	network.lldp_med.interval		
-----------------	---------------------------	--	--

Description:	Sets the LLDP-MED packet interval (in seconds).		
---------------------	---	--	--

Values:	1–30	Default:	30
----------------	------	-----------------	----

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:	<code>network.eapol.access_password</code>		
Description:	Sets the 802.1x EAPOL MD5 password.		
Values:	Text string	Default:	Blank

Setting:	<code>network.vendor_class_id</code>		
Description:	Sets the vendor ID for DHCP option 60.		
Values:	Text string	Default:	Vtech Vesa VDP650

Setting:	<code>network.user_class</code>		
Description:	Sets the user class for DHCP option 77.		
Values:	Text string	Default:	Vtech Vesa VDP650

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:	<code>network.ip.pppoe.service_name</code>		
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:	<code>network.ip.pppoe.username</code>		
Description:	If IPv4 mode is PPPoE, enter your PPPoE account username.		
Values:	Text string	Default:	Blank
Setting:	<code>network.ip.pppoe.access_password</code>		
Description:	If IPv4 mode is PPPoE, enter your PPPoE account password.		
Values:	Text string	Default:	Blank
Setting:	<code>network.ip6.mode</code>		
Description:	Set the IPv6 network mode, depending on how the device will be assigned an IP address.		
Values:	disable, auto, static	Default:	disable
Setting:	<code>network.ip.static_ip6_addr</code>		
Description:	When IPv6 mode is static, enter the static IP address for the network.		
Values:	Text string (IPv6)	Default:	Blank
Setting:	<code>network.ip6.prefix</code>		
Description:	When IPv6 mode is static, enter the IPv6 address prefix length.		
Values:	0–128	Default:	64
Setting:	<code>network.ip6.gateway_addr</code>		
Description:	When IPv6 mode is static, enter the default gateway address.		
Values:	Text string (IPv6)	Default:	Blank

Setting:	<code>network.ip6.dns1</code>		
Description:	If manual DNS configuration is enabled, enter the address for the primary DNS server.		
Values:	Text string (IPv6)	Default:	Blank

Setting:	<code>network.ip6.dns2</code>		
Description:	If manual DNS configuration is enabled, enter the address for the secondary DNS server.		
Values:	Text string (IPv6)	Default:	Blank

Setting:	<code>network.ip6.manually_configure_dns</code>		
Description:	Enable or disable manual DNS configuration for IPv6.		
Values:	0 (disable), 1 (enable)	Default:	0

Setting:	<code>network.vpn.enable</code>		
Description:	Enables or disables the phone to connect using the OpenVPN client. For more information, see “VPN” on page 69 .		
Values:	0 (disable), 1 (enable)	Default:	0

"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 VDP650.

General configuration file settings

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,	Default:	config_and_firmware
	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:	<code>provisioning.remote_check_sync_enable</code>		
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:	<code>provisioning.crypto_enable</code>		
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:	<code>provisioning.crypto_passphrase</code>		
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:	<code>provisioning.check_trusted_certificate</code>		
Description:	Enables or disables accepting only a trusted TLS certificate for access to the provisioning server.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>provisioning.pnp_enable</code>		
Description:	Enables or disables the VDP650 checking for the provisioning URL using the Plug-and-Play Subscribe and Notify protocol.		
Values:	0 (disabled), 1 (enabled)	Default:	1
Setting:	<code>provisioning.pnp_response_timeout</code>		
Description:	Sets how long the VDP650 repeats the SUBSCRIBE request if there is no reply from the PnP server.		
Values:	1–60	Default:	10

Setting:	<code>provisioning.pwd_export_enable</code>		
Description:	Enables or disables passwords from being exported in plain text. This parameter is not available on the WebUI. The passwords affected are: <ul style="list-style-type: none">■ <code>network.eapol.access_password</code>■ <code>provisioning.fw_server_access_password</code>■ <code>provisioning.server_access_password</code>■ <code>profile.admin.access_password</code>■ <code>profile.user.access_password</code>■ <code>sip_account.x.authentication_access_password</code>■ <code>remoteDir.ldap_access_password</code>■ <code>remoteDir.broadsoft_access_password</code>		
Values:	0 (disabled), 1 (enabled)	Default:	0

MAC-specific configuration file settings

Setting:	<code>provisioning.firmware_url</code>		
Description:	Sets the URL for the server hosting the firmware file.		
Values:	Text string	Default:	Blank

Setting:	<code>provisioning.handset_firmware_url</code>		
Description:	Sets the URL for the server hosting the handset firmware file.		
Values:	Text string	Default:	Blank

Setting:	<code>provisioning.cordless_deskset_firmware_url</code>		
Description:	Sets the URL for the server hosting the cordless deskset firmware file.		
Values:	Text string	Default:	Blank

Setting:	<code>provisioning.fw_server_username</code>		
Description:	Sets the authentication name for the server hosting the firmware file.		
Values:	Text string	Default:	Blank

Setting:	<code>provisioning.fw_server_access_password</code>		
Description:	Sets the authentication password for the server hosting the firmware file.		
Values:	Text string	Default:	Blank

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

Setting:	<code>provisioning.server_username</code>		
Description:	Sets the authentication name for the provisioning server.		
Values:	Text string	Default:	Blank

Setting:	<code>provisioning.server_access_password</code>		
Description:	Sets the authentication password for the provisioning server.		
Values:	Text string	Default:	Blank

"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 VDP650.

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

Setting: time_date.ntp_server

Description: Enables or disables NTP server to set time and date.

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

Setting: time_date.ntp_server_addr

Description: Sets the URL for the NTP server.

Values: IPv4, IPv6 or FQDN **Default:** us.pool.ntp.org

Setting: time_date.ntp_dhcp_option

Description: Enables or disables DHCP option 42 to find the NTP server.

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

Setting: time_date.selected_timezone

Description: Sets the local timezone.

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

Setting:	<code>time_date.daylight_saving_auto_adjust</code>		
Description:	Sets the device to automatically adjust clock for daylight savings.		
Values:	0 (disabled), 1 (enabled)	Default:	1
Setting:	<code>time_date.daylight_saving_user_defined</code>		
Description:	Enables or disables manual daylight savings configuration.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>time_date.daylight_saving_start_month</code>		
Description:	Sets the month that daylight savings time starts.		
Values:	January–December	Default:	March
Setting:	<code>time_date.daylight_saving_start_week</code>		
Description:	Sets the week that daylight savings time starts.		
Values:	1–5	Default:	2
Setting:	<code>time_date.daylight_saving_start_day</code>		
Description:	Sets the day that daylight savings time starts.		
Values:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	Default:	Sunday
Setting:	<code>time_date.daylight_saving_start_hour</code>		
Description:	Sets the hour that daylight savings time starts.		
Values:	00:00–23:00	Default:	02:00
Setting:	<code>time_date.daylight_saving_end_month</code>		
Description:	Sets the month that daylight savings time ends.		
Values:	January–December	Default:	November

Setting:	<code>time_date.daylight_saving_end_week</code>		
Description:	Sets the week that daylight savings time ends.		
Values:	1–5	Default:	1
Setting:	<code>time_date.daylight_saving_end_day</code>		
Description:	Sets the day that daylight savings time ends.		
Values:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	Default:	Sunday
Setting:	<code>time_date.daylight_saving_end_hour</code>		
Description:	Sets the hour that daylight savings time ends.		
Values:	00:00–23:00	Default:	02:00
Setting:	<code>time_date.daylight_saving_amount</code>		
Description:	Sets the daylight savings time offset in minutes.		
Values:	0–255	Default:	60
Setting:	<code>time_date.timezone_dhcp_option</code>		
Description:	Enables or disables DHCP option 2/100/101 for determining time zone information.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>time_date.ntp_server_update_interval</code>		
Description:	Sets the delay between NTP server updates, in seconds.		
Values:	0–4294967295	Default:	1000
Setting:	<code>time_date.time_and_date</code>		
Description:	Manually sets the date and time. Use the format <year>-<month>-<day>T<hour>:<minute>:<second>		
Values:	<year>-<month>-<day>T<hour>:<minute>:<second>	Default:	2016-03-01T12:00:00

"log" Module: Log Settings

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

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

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

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

Setting:	log.syslog_enable
-----------------	-------------------

Description:	Enables or disables log output to syslog server.
---------------------	--

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

Setting:	log.syslog_server_address
-----------------	---------------------------

Description:	Sets the syslog server IP address.
---------------------	------------------------------------

Values:	Text string (IPv4 or IPv6)	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 VDP650.

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

Setting:	remoteDir.ldap_enable		
Description:	Enables or disables the VDP650 4-Line base station's access to the LDAP directory.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	remoteDir.ldap_directory_name		
Description:	Sets the LDAP directory name.		
Values:	Text string	Default:	Blank
Setting:	remoteDir.ldap_server_address		
Description:	Sets the LDAP server IP address.		
Values:	Text string	Default:	Blank
Setting:	remoteDir.ldap_port		
Description:	Sets the LDAP server port.		
Values:	1–65535	Default:	389
Setting:	remoteDir.ldap_protocol_version		
Description:	Sets the LDAP protocol version.		
Values:	version_2, version_3	Default:	version_3
Setting:	remoteDir.ldap_authentication_type		
Description:	Sets the LDAP authentication type.		
Values:	simple, ssl	Default:	simple

Setting:	<code>remoteDir.ldap_user_name</code>		
Description:	Sets the LDAP authentication user name.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_access_password</code>		
Description:	Sets the LDAP authentication password.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_base</code>		
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:	<code>remoteDir.ldap_max_hits</code>		
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:	<code>remoteDir.ldap_search_delay</code>		
Description:	Sets the LDAP maximum search delay in seconds.		
Values:	0–500	Default:	0
Setting:	<code>remoteDir.ldap_firstname_filter</code>		
Description:	Sets the LDAP first name attribute filter.		
Values:	Text string	Default:	Firstname
Setting:	<code>remoteDir.ldap_lastname_filter</code>		
Description:	Sets the LDAP last name attribute filter.		
Values:	Text string	Default:	Lastname

Setting:	<code>remoteDir.ldap_number_filter</code>		
Description:	Sets the LDAP number filter.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_firstname_attribute</code>		
Description:	Sets the name attributes. Enter the name attributes that you want the VDP650 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:	<code>remoteDir.ldap_lastname_attribute</code>		
Description:	Sets the last name attributes.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_work_number_attributes</code>		
Description:	Sets the number attributes. Enter the number attributes that you want the VDP650 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:	<code>remoteDir.ldap_mobile_number_attributes</code>		
Description:	Sets the mobile number attributes.		
Values:	Text string	Default:	Blank
Setting:	<code>remoteDir.ldap_other_number_attributes</code>		
Description:	Sets the “other” number attributes.		
Values:	Text string	Default:	Blank

Setting:	<code>remoteDir.ldap_incall_lookup_enable</code>		
Description:	Enables or disables LDAP incoming call lookup. If enabled, the VDP650 searches the LDAP directory for the incoming call number. If the number is found, the VDP650 uses the LDAP entry for CID info.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>remoteDir.ldap_outcall_lookup_enable</code>		
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:	<code>remoteDir.xml.x.name</code>		
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:	<code>remoteDir.xml.x.uri</code>		
Description:	The location of the XML directory file, from which the phone will sync and retrieve directory entries.		
Values:	URI	Default:	Blank
Setting:	<code>remoteDir.xml.x.call_lookup_enable</code>		
Description:	Enables/disables the call lookup feature for incoming and outgoing calls.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>remoteDir.xml.x.contact_entry_tag</code>		
Description:	Sets the tag name for directory entry.		
Values:	Text string	Default:	DIR_ENTRY
Setting:	<code>remoteDir.xml.x.first_name_tag</code>		
Description:	Sets the first name tag for a directory entry.		
Values:	Text string	Default:	DIR_ENTRY_NAME_FIRST

Setting:	<code>remoteDir.xml.x.last_name_tag</code>		
Description:	Sets the last name tag for a directory entry.		
Values:	Text string	Default:	DIR_ENTRY_NAME_LAST

Setting:	<code>remoteDir.xml.x.work_number_tag</code>		
Description:	Sets the work number tag for a directory entry.		
Values:	Text string	Default:	DIR_ENTRY_NUMBER_WORK

Setting:	<code>remoteDir.xml.x.mobile_number_tag</code>		
Description:	Sets the mobile number tag for a directory entry.		
Values:	Text string	Default:	DIR_ENTRY_NUMBER_MOBILE

Setting:	<code>remoteDir.xml.x.other_number_tag</code>		
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

“trusted_ip” Module: Trusted IP Settings

The trusted_ip settings provide enhanced security for the VDP650. 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 100 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 settings provide enhanced security for the VDP650. When enabled, these settings can filter network traffic and reject any traffic from unauthorized sources.

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

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

Setting:	<code>trusted_ip.only_accept_sip_account_servers</code>		
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 VDP650 user. These settings are useful for initial setup. You may wish to remove these settings from auto-provisioning update files so that users do not have their own settings overwritten.

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

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

Setting:	<code>user_pref.web_language</code>
-----------------	-------------------------------------

Description:	Sets the language that appears on the WebUI.
---------------------	--

Values:	en, fr, es	Default:	en
----------------	------------	-----------------	----

Setting:	<code>user_pref.call_terminated.busy_tone_enable</code>
-----------------	---

Description:	Enables the VDP650 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:	<code>user_pref.account.x.diversion_display</code>
-----------------	--

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
----------------	---------------------------	-----------------	---

"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 8.

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

Setting:	<code>call_settings.account.x.block_anonymous_enable</code>
-----------------	---

Description:	Enables or disables anonymous call blocking.
---------------------	--

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

Setting:	<code>call_settings.account.x.outgoing_anonymous_enable</code>
-----------------	--

Description:	Enables or disables outgoing anonymous calls.
---------------------	---

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

Setting:	<code>call_settings.account.x.dnd_enable</code>
-----------------	---

Description:	Enables or disables Do Not Disturb for account x.
---------------------	---

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

Setting:	<code>call_settings.account.x.call_fwd_always_enable</code>
-----------------	---

Description:	Enables or disables Call Forward Always for account x.
---------------------	--

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

Setting:	<code>call_settings.account.x.call_fwd_always_target</code>
-----------------	---

Description:	Sets the Call Forward Always target number for account x.
---------------------	---

Values:	Text string	Default:	Blank
----------------	-------------	-----------------	-------

Setting:	<code>call_settings.account.x.call_fwd_busy_enable</code>
-----------------	---

Description:	Enables or disables Call Forward Busy for account x.
---------------------	--

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

Setting:	<code>call_settings.account.x.call_fwd_busy_target</code>		
Description:	Sets the Call Forward Busy target number for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>call_settings.account.x.cfna_enable</code>		
Description:	Enables or disables Call Forward No Answer for account x.		
Values:	0 (disabled), 1 (enabled)	Default:	0
Setting:	<code>call_settings.account.x.cfna_target</code>		
Description:	Sets the Call Forward No Answer target number for account x.		
Values:	Text string	Default:	Blank
Setting:	<code>call_settings.account.x.cfna_delay</code>		
Description:	Sets the Call Forward No Answer delay (in number of rings) for account x.		
Values:	1–10	Default:	6

“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:	<code>audio.x.jitter_mode</code>		
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:	<code>audio.x.fixed_jitter.delay</code>		
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:	<code>audio.x.adaptive_jitter.min_delay</code>		
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:	<code>audio.x.adaptive_jitter.target_delay</code>		
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:	<code>audio.x.adaptive_jitter.max_delay</code>		
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:	<code>audio.x.rtp.port_start</code>		
Description:	Sets the Local RTP port range start.		
Values:	1–65535	Default:	18000

Setting:	<code>audio.x.rtp.port_end</code>		
Description:	Sets the Local RTP port range end.		
Values:	1–65535	Default:	19000

Setting:	<code>audio.rtcp_xr.enable</code>		
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

"file" Module: Imported File Settings

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

- Contact lists
- Security certificates

The following certificates are supported:

- Per-account TLS certificate (you can choose to use the Account 1 certificate for all accounts)
- LDAP
- Web server (the VDP650 has a default self-signed web server certificate)
- Provisioning
- Languages

File parameter values are URLs that direct the VDP650 to the location of the file to be imported.

None of these settings are exported when you manually export the configuration from the VDP650.

General configuration file settings

Setting:	<code>file.certificate.x.url</code>		
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:	<code>file.protected_certificate.x.url</code>		
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:	<code>file.certificate.trusted.url</code>		
Description:	URL to upload a trusted certificate file in pem or crt. It will be given the first available index and marked as unprotected. For example, <code><protocol>://<user>:<password>@<host>:<port>/<url-path></code>		
Values:	Text string	Default:	Blank

Setting:	<code>file.protected_certificate.trusted.url</code>		
Description:	URL to upload a trusted certificate file in pem or crt. It will be given the first available index and marked as protected. For example, <code><protocol>://<user>:<password>@<host>:<port>/<url-path></code>		
Values:	Text string	Default:	Blank
Setting:	<code>file.protected_certificate.custom_device.url</code>		
Description:	URL to upload a custom device certificate to override the factory installed device certificate. For example, <code><protocol>://<user>:<password>@<host>:<port>/<url-path></code>		
Values:	Text string	Default:	Blank
Setting:	<code>file.action</code>		
Description:	<p>Enables you to delete certain certificates.</p> <ul style="list-style-type: none"> ■ <code>removecertificate_customdevice</code>: remove the custom device certificate and resume the use of the factory installed device certificate ■ <code>removecertificate_allnonprotected</code>: remove all non-protected trusted certificates ■ <code>removecertificate_all</code>: remove the custom device certificate and all protected or non-protected trusted certificates <p>Enables you to delete a custom language from the WebUI, the deskset screens, or both.</p>		
Values:	<code>removecertificate_</code> <code>customdevice</code> , <code>removecertificate_</code> <code>allnonprotected</code> , <code>removecertificate_all</code> <code>removecustomlanguage_all</code> , <code>removecustomlanguage_webui</code>	Default:	Blank

Setting:	file.		
Description:			
Values:	Text string	Default:	Blank

Setting:	file.vpn.advanced_config		
Description:	URL of OpenVPN client configuration file. For more information, see “VPN” on page 69 .		
Values:	Text string	Default:	Blank

MAC-specific configuration file settings

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

“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:	<code>tr069.enable</code>
-----------------	---------------------------

Description:	Enable/disable the TR-069 subsystem.
---------------------	--------------------------------------

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

Setting:	<code>tr069.acs.url</code>
-----------------	----------------------------

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

Values:	Text string	Default:	Blank
----------------	-------------	-----------------	-------

Setting:	<code>tr069.acs.username</code>
-----------------	---------------------------------

Description:	Enter user name for ACS authentication.
---------------------	---

Values:	Text string	Default:	Blank
----------------	-------------	-----------------	-------

Setting:	<code>tr069.acs.access_password</code>
-----------------	--

Description:	Enter password for ACS authentication.
---------------------	--

Values:	Text string	Default:	Blank
----------------	-------------	-----------------	-------

Setting:	<code>tr069.periodic_inform.enable</code>
-----------------	---

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

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

Setting:	<code>tr069.periodic_inform.interval</code>
-----------------	---

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

Values:	1–65535	Default:	3600
----------------	---------	-----------------	------

Setting:	<code>tr069.connection_request.username</code>		
Description:	Set the user name for authenticating the connection sent from the ACS.		
Values:	Text string	Default:	Blank

Setting:	<code>tr069.connection_request.access_password</code>		
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 a string of 12 elements separated by a space:

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

Where:

<num of freq>: 0-4

<freq1>: 0-65535

<amp1>: -32768-32767

<freq2>: 0-65535

<amp2>: -32768-32767

<freq3>: 0-65535

<amp3>: -32768-32767

<freq4>: 0-65535

<amp4>: -32768-32767

<on duration>: 0-2³²

<off duration>: 0-2³²

<repeat count>: 0-65535

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

Setting:	tone.inside_dial_tone.num_of_elements		
-----------------	---------------------------------------	--	--

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

Values:	1-5	Default:	1
----------------	-----	-----------------	---

Setting:	tone.inside_dial_tone.element.1		
-----------------	---------------------------------	--	--

Description:	Defines the inside dial tone element 1.		
---------------------	---	--	--

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

Setting:	tone.inside_dial_tone.element.x		
Description:	Defines the inside dial tone element x.		
Values:	Tone element string	Default:	Blank
Setting:	tone.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.		
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 0 375 375 65535
Setting:	tone.busy_tone.element.x		
Description:	Defines the busy tone element x.		
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.		
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.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.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

"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:	<code>profile.admin.access_password</code>		
Description:	Sets the administrator password for accessing the admin menus on the VDP651 and the WebUI.		
Values:	Text string (15 characters maximum)	Default:	admin

MAC-specific configuration file settings

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

CHAPTER 6

TROUBLESHOOTING

If you have difficulty with your VDP650 4-Line base station, please try the suggestions below.

**NOTE**

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

Common Troubleshooting Procedures

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

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

- Ensure the handset is fully charged and in the charger. Remove and replace the handset in its charger before selecting **Register** on the VDP650.
- Ensure the handset is not already registered to another base. If it has been registered to another base, deregister it.

The firmware upgrade or configuration update isn't working.

- Before using the WebUI, ensure you have the latest version of your web browser installed. Some menus and controls in older browsers may operate differently than described in this manual.
- Ensure you have specified the correct path to the firmware and configuration files on the **SERVICING > Firmware Upgrade > Auto Upgrade** page and the **SERVICING > Provisioning** page.

- If the phone is not downloading a MAC-specific configuration file, ensure the filename is all upper case.

Provisioning: "Use DHCP Option" is enabled, but the VDP650 is not getting a provisioning URL from the DHCP Server.

- Ensure that DHCP is enabled in Network settings.

APPENDIXES

Appendix A: Maintenance

Taking care of your products

- Your VDP650 4-Line base station contains sophisticated electronic parts, so you must treat it with care.
- Avoid rough treatment.
- Place the handset down gently.
- Save the original packing materials to protect your VDP650 4-Line base station if you ever need to ship it.

Avoid water

- You can damage your VDP650 4-Line base station if it gets wet. Do not use the handset in the rain, or handle it with wet hands. Do not install the VDP650 4-Line base station near a sink, bathtub or shower.

Electrical storms

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

Cleaning your products

- Your VDP650 4-Line base station has a durable plastic casing that should retain its luster for many years. Clean it only with a soft cloth slightly dampened with water or a mild soap.
- Do not use excess water or cleaning solvents of any kind.

Remember that electrical appliances can cause serious injury if used when you are wet or standing in water. If the VDP650 4-Line base station should fall into water, DO NOT RETRIEVE IT UNTIL YOU UNPLUG THE POWER CORD AND NETWORK CABLE FROM THE WALL, then pull the unit out by the unplugged cords.

Appendix B: GPL License Information

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

VTech Communications, Inc.,
9590 SW Gemini Drive, Suite 120
Beaverton OR 97008
ATTN: Information Technology Group—VDP650 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.

