Installing & Configuring Pingtel phones

- Pingtel xpressa™
- Pingtel instant xpressa™

Version 1.2
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Feature overview</td>
<td>1</td>
</tr>
<tr>
<td>Operating system</td>
<td>2</td>
</tr>
<tr>
<td>Java support</td>
<td>2</td>
</tr>
<tr>
<td>Browser-based access</td>
<td>3</td>
</tr>
<tr>
<td>Installation objectives</td>
<td>4</td>
</tr>
<tr>
<td>Making peer-to-peer calls</td>
<td>5</td>
</tr>
<tr>
<td>Implementing SIP servers</td>
<td>7</td>
</tr>
<tr>
<td>Using the pingtel.net calling service</td>
<td>8</td>
</tr>
<tr>
<td>Other Pingtel products</td>
<td>8</td>
</tr>
<tr>
<td>instant xpressa softphone</td>
<td>9</td>
</tr>
<tr>
<td>xpressa Development Kit (xDK)</td>
<td>9</td>
</tr>
<tr>
<td>Pingtel Deployment Server (PDS)</td>
<td>9</td>
</tr>
<tr>
<td>Support services</td>
<td>10</td>
</tr>
<tr>
<td>Documentation resources</td>
<td>10</td>
</tr>
<tr>
<td>Using <a href="http://www.pingtel.com">www.pingtel.com</a></td>
<td>10</td>
</tr>
<tr>
<td>Contacting Pingtel</td>
<td>11</td>
</tr>
<tr>
<td><strong>Installing an xpressa phone</strong></td>
<td>12</td>
</tr>
<tr>
<td>Initial assembly</td>
<td>13</td>
</tr>
<tr>
<td>xpressa phone power sources</td>
<td>13</td>
</tr>
<tr>
<td>Wall outlet</td>
<td>13</td>
</tr>
<tr>
<td>Cisco® switch or Inline Power patch panel</td>
<td>14</td>
</tr>
<tr>
<td>Installing with power from the PIM</td>
<td>14</td>
</tr>
<tr>
<td>Installing with Inline Power</td>
<td>15</td>
</tr>
<tr>
<td>xpressa phone startup</td>
<td>16</td>
</tr>
</tbody>
</table>
Contents

Assigning network settings 18
   Dynamic (DHCP) network settings 18
   Identifying a DNS server 19
   Static network settings 20
   Setting static network values 20
   Verifying network settings 22
   Switching from static to DHCP 23

Configuring an xpressa phone 24
   Configuration interfaces 24
   Using the phonetop interface 25
   Using the browser-based interface 26
   Using the MyPingtel user portal 28
   Configuration files 28
      Editing configuration files manually 29
      Reviewing configuration files 34

Using administrative security features 38
   Protected tasks 38
      On the phonetop 38
         With the browser-based interface 39
   Administrative log on 39
      Logging on to the phonetop 40
      Logging on to the browser-based interface 40
   Change the administrative password 41
      Changing the password on the phonetop 41
      Changing the password with a browser 42
   Reset the administrative password 43
   Set up users for the browser-based interface 44

Basic configuration 46
   Set parameters for dialing 46
### Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning a unique extension</td>
<td>46</td>
</tr>
<tr>
<td>Automating dialing</td>
<td>47</td>
</tr>
<tr>
<td>Defining digit maps</td>
<td>48</td>
</tr>
<tr>
<td>Secure xpressa phones</td>
<td>54</td>
</tr>
<tr>
<td>Set call handling parameters</td>
<td>55</td>
</tr>
<tr>
<td>Selecting incoming call alerts</td>
<td>56</td>
</tr>
<tr>
<td>Setting up call forwarding</td>
<td>57</td>
</tr>
<tr>
<td>Defining call waiting or forward on busy</td>
<td>58</td>
</tr>
<tr>
<td>Setting up Do Not Disturb</td>
<td>59</td>
</tr>
<tr>
<td>Define time-related parameters</td>
<td>61</td>
</tr>
<tr>
<td>Specifying a time server</td>
<td>61</td>
</tr>
<tr>
<td>Setting the time to display</td>
<td>61</td>
</tr>
<tr>
<td>Set network management parameters</td>
<td>63</td>
</tr>
<tr>
<td>Controlling browser access</td>
<td>63</td>
</tr>
<tr>
<td>Enabling voice mail message waiting indication</td>
<td>65</td>
</tr>
<tr>
<td>Sending SNMP messages</td>
<td>67</td>
</tr>
<tr>
<td>Selecting an Ethernet duplex mode</td>
<td>69</td>
</tr>
<tr>
<td>Define an image for the home screen</td>
<td>70</td>
</tr>
<tr>
<td><strong>Setting up Pingtel SIP phone environments</strong></td>
<td><strong>71</strong></td>
</tr>
<tr>
<td>SIP servers</td>
<td>71</td>
</tr>
<tr>
<td>Registry server</td>
<td>72</td>
</tr>
<tr>
<td>Directory server</td>
<td>73</td>
</tr>
<tr>
<td>Proxy server</td>
<td>77</td>
</tr>
<tr>
<td>Redirect server</td>
<td>77</td>
</tr>
<tr>
<td>Call addressing</td>
<td>78</td>
</tr>
<tr>
<td>Dialing a SIP URL</td>
<td>79</td>
</tr>
<tr>
<td>Dialing speed dial numbers</td>
<td>79</td>
</tr>
<tr>
<td>Dialing extensions and telephone numbers</td>
<td>80</td>
</tr>
<tr>
<td>Routing calls through additional servers</td>
<td>82</td>
</tr>
</tbody>
</table>

Copyright © 2001 Pingtel Corp.  
Version 1.2  
Page v
## Contents

### Configuring phones for SIP environments
- Identify SIP servers 85
- Defining the SIP Location server 85
- Setting up SIP registration 86
- Defining an additional Proxy server 87
- SIP messaging parameters 87
  - Defining ports for SIP messages 88
  - Enabling session timer 88
- Authentication parameters 88
  - Setting up authentication for outgoing calls 89
  - Authenticating incoming calls 92

### Working with firewalls and NAT
- Configure the firewall 94
  - Recording the external IP address 94
  - Opening VoIP ports 94
- Configure the xpressa phone 95
  - Identifying the external IP address 96
  - Setting the SIP port 96
  - Setting the RTP/RTCP ports 96
- Work with a firewall with NAT 97
  - Work with a proxied firewall 99
    - Configuring phones for a SIP firewall proxy 99
    - Using HTTP proxy settings 99

### Supporting QoS techniques
- TOS bit markings 101
- VLAN 802.1p prioritization 102
- RTP/RTCP ports 103

### Configuring phones for pingtel.net calling
- xpressa phone sign in 104
Contents

Signing in to pingtel.net 105
Signing out of pingtel.net 105
pingtel.net service parameters 106

Managing xpressa phones 107
  Install software upgrades 107
    Installing upgrades automatically with VersionCheck 108
    Installing upgrades manually 108
  Manage xpression applications 111
    Reviewing an app-config file 112
    Editing an app-config file 112
    Uploading an edited app-config file 113
  Restart an xpressa phone 113
    Restarting from the phonetop 113
    Restarting manually 114
    Restarting from a browser 115
  Revert to factory defaults 115
  Install audio files 117

Troubleshooting 119
  Support checklists 119
    No dial tone 119
    LCD display screen is blank 120
    Buttons do not light or work 120
    Problems with incoming calls 121
    Problems with outgoing calls 123
    One-way conversation 124
    No access to browser-based interface 125
    Connection is noisy 126
    xpression applications don’t load or run 126
    Physical defects 127
  Troubleshooting tools 128
Contents

Using the SIP message log 128
Setting configuration parameters for troubleshooting 141
Using the upgrade log 142
Reviewing the file list 143
Review configuration files 144
What to look for in manually edited files 144
Printing a configuration file 145
Contact Pingtel's TAC 145

FCC information 147

Appendix A: Session Initiation Protocol 148
SIP messages 148
Methods 149
Response codes 150
Message headers 151
Sample SIP message 151
Message flow examples 152
SIP addresses 155
SIP transactions 155
SIP sessions 156
SIP calls 156
System components 156
Supported SIP features 158

Appendix B: Parameter reference 160

Appendix C: Alphabetical parameter index 185

Index 188
Introduction

This guide describes installation and configuration procedures for Pingtel xpressa™ phones. The tasks described in this guide affect the ability of xpressa phones to function in your network.

This section presents:
• The intended audience of this guide.
• Features of Pingtel xpressa phones.
• Different xpressa phone installations.
• Pingtel products that can be used with the xpressa phone.
• Pingtel’s support services and documentation resources.

Audience

In general, the tasks described in this guide should be performed by a system administrator or network engineer with an understanding of networking and telephony concepts, or by an xpressa phone user working under the direction of such an administrator or engineer.

Using Pingtel phones is written for all xpressa phone users.

Feature overview

Pingtel’s xpressa phone is a fully-featured telephone that offers all the features of a traditional telephone. It is also a VoIP (Voice over IP) IP telephone that can be plugged directly into an IP network, and a user agent for sending and receiving SIP (Session Initiation Protocol) messages.

Tip For background information on SIP see page 148.
Introduction

In contrast to the phones in traditional telephone systems, the xpressa phone was designed with the Internet as its architectural model. As a result, an xpressa phone works like a PC: it provides an open, extensible platform for delivering features and functionality. It does not depend on other devices to offer services the way a PSTN telephone or terminal does.

To be an intelligent endpoint, each xpressa phone includes:

- An operating system
- Support for Java™ programs
- An embedded web server

An xpressa phone’s memory and CPU allow you to install and run applications directly on the phone. For memory and CPU specifications, see the model description for your xpressa phone.

Operating system

xpressa phones use the VxWorks® operating system. VxWorks is a flexible, scalable, reliable, and commercially proven real-time operating system (RTOS).

Java support

PersonalJava 3.0, a product of Sun Microsystems, Inc., runs on xpressa phones and offers a fully featured Java platform. The xpressa phone is an open platform; third party developers can develop applications in the Java object-oriented programming language.

Applications for the xpressa phone are called xpression™ applications. An xpression is packaged in a Java .JAR file that is stored on an external web site or a web server in your local network. Adding xpression applications to an xpressa phone can help users perform basic phone tasks more efficiently or expand the xpressa phone’s capabilities.
Feature overview

Pingtel’s xpressa Development Kit™ (xDK) provides tools to help third party developers build, test, and deploy xpression applications. For more information on using the xDK see The xpressa Development Kit™ Programmer’s Guide.

Browser-based access

In addition to the user interface available from an xpressa phone’s phonetop, every xpressa phone has an embedded web server. This web server delivers web pages with information about the phone to an HTML browser on a PC. The embedded web server of an xpressa phone can be enabled and disabled as needed; see PHONESET_HTTP_PORT on page 64.

Tip The User interface fundamentals section in Using Pingtel phones provides “how to” information on the phonetop interface, the browser-based interface, and the MyPingtel user portal.

Browser-based interface

The browser-based user interface offers the use of a PC keyboard and monitor for performing configuration, maintenance, call control, and troubleshooting tasks on an xpressa phone. To access the embedded web server of an xpressa phone, you enter the phone’s IP address as the location or address in a web browser on any networked PC. Both administrators and users can use the xpressa phone’s browser-based interface to maintain individual xpressa phones.

Tip xpressa phones provide password protection for access to the browser-based interface. For more information see page 38.
Introduction

**MyPingtel user portal**

Another PC-based interface provides access to user-oriented features: the MyPingtel™ user portal. xpressa phone users can navigate to Pingtel’s http://my.pingtel.com web site from any web browser and register for access to data provided by Pingtel about xpression applications, services, and other news.

Registering a Pingtel phone with the MyPingtel user portal provides users with another interface option to perform tasks like making calls, defining speed dial numbers, installing xpression applications, and setting call handling preferences.

**Tip** The MyPingtel user portal requires a two-step registration process. The user:

1. Visits http://my.pingtel.com to obtain a user name and password
2. Registers a phone to permit access to its embedded web server.

For more information see Using Pingtel phones.

**Installation objectives**

When you install xpressa phones as part of your Ethernet/LAN environment, your objective may be to evaluate the phones or xpression applications, to deploy the phones in a complete SIP environment, or to make trial calls with a VoIP calling service. The configuration procedures that you will follow vary based on your objective:

- To evaluate or test a small number of xpressa phones in a lab environment, you can make peer-to-peer calls between the xpressa phones in your organization after minimal set up.
- To deploy xpressa phones in production or for larger trials, you implement SIP servers and identify each xpressa phone with a unique extension. This type of installation requires a SIP Directory server and,
Installation objectives

potentially, a SIP Registry server. SIP servers can be deployed within your own IP network, or you may use the services of a SIP telecommuni-
cations service provider that offers access to SIP servers on a hosted basis.

• If you need to make calls either to SIP phones that are outside your immediate network or to traditional PSTN telephones on a trial basis, you can use Pingtel’s pingtel.net™ calling service.

To help you use this guide to meet your objectives, an overview of each type of installation follows.

Making peer-to-peer calls

Before you make peer-to-peer calls between xpressa phones you perform the following setup tasks:

• Install the xpressa phones as described on page 12.
• Verify that your DHCP server has assigned network settings to the xpressa phones, or set static network values yourself. See Assigning network settings on page 18.

When you complete these tasks, you can make calls from one xpressa phone to another by dialing the destination phone’s assigned IP address as its SIP URL.

Find an IP address

1 From an xpressa phone’s home screen press MORE and select the Menu tab.
2 Press About.
Introduction

3 Press Info.
   The phone's IP address displays on the second line.

![Phone Information]

4 Press OK to return to the xpressa phone's home screen.

Make a call

1 From an xpressa phone's home screen press Dial by URL.

![Dialing]

2 Use the dial pad to enter the destination phone's IP address.
   For example, to dial a phone with an IP address of 10.1.1.111, enter 10.1.1.111.

3 Press Dial.
   For more information see Using the xpressa phone in Using Pingtel phones.
Implementing SIP servers

To create a complete, production-level environment that includes xpressa phones, you set up SIP servers (or contract for their use from a SIP telecommunications service provider) and configure the phones with information about the SIP environment. SIP servers provide call setup and tear-down services to the users of your phone environment. They may also provide services such as dynamically mapping telephone numbers to xpressa phone IP addresses, or collecting system-level accounting information.

You may also need additional servers such as voice mail servers to create a complete telecommunications system. Like the SIP servers, additional servers may be located on your IP network or provided by third-party hosted IP voice service providers.

- Install the xpressa phones as described on page 12.
- Verify network settings assigned to each phone by a DHCP server, or set static network values. See page 18.
- Set up or identify the SIP Directory server that will provide location services for addressing calls. See page 73.
  Optionally, you can identify a SIP Registry server or SIP Proxy firewall server. See page 72.
- Configure the xpressa phones:
  - Assign a unique identifying extension to each phone. See page 46.
  - Assign the addresses of your SIP servers to each xpressa phone as described on page 85.
- Optionally, configure xpressa phones to use your voice mail server:
  - To set up the voice mail server as the call forwarding address for busy or unanswered calls, see page 57.
  - To provide simple access to the voice mail server for message retrieval, see page 66.
Introduction

For more information on SIP environments see page 71.

Using the pingtel.net calling service

The pingtel.net calling service is a test network that provisions an xpressa phone to make calls to PSTN phones and to xpressa phones that are outside your network. This service also supports inbound calls to an xpressa phone from PSTN and xpressa phones.

To use this service with an xpressa phone, you:

1. Register for Pingtel’s AppDev Zone at http://appdev.pingtel.com on the Internet. You receive e-mail with your user name and assigned password.

2. Sign up for the calling service: click Services on an AppDev Zone web page. This procedure provisions a specific xpressa phone for use with the service. You receive e-mail with your xpressa phone’s assigned extension or telephone number.

3. Install the xpressa phone as described on page 12.

4. Follow the instructions on page 104 to start using the pingtel.net service on the xpressa phone.

Tip When you sign up to use the pingtel.net service, you provide data about your network environment. The service supplies this data back to your phone in a configuration file. For this type of installation, further configuration is not required.

Other Pingtel products

In addition to its xpressa phone, Pingtel offers the instant xpressa™ softphone and the xpressa Development Kit. Release of the Pingtel Deployment Server™ (PDS) is planned for a future date.
instant xpressa softphone

The instant xpressa softphone is a software application that can be installed on a PC with a sound card, microphone, and speakers. Like Pingtel’s xpressa phone, the instant xpressa softphone is a Java VoIP phone.

Tip This guide uses “xpressa phone” to indicate either the xpressa phone appliance or the instant xpressa softphone. See the Appendix to Using Pingtel phones for differences between instant xpressa and an xpressa phone.

xpressa Development Kit (xDK)

The xpressa Development Kit provides tools for programmers to build, test, and deploy xpression applications for the xpressa phone. The xDK includes the instant xpressa softphone.

Pingtel Deployment Server (PDS)

Pingtel plans a future release of its PDS, a configuration server application that runs on a server computer. The architecture of xpressa phones supports remote configuration from a networked PDS to allow for centralized and secure management of large numbers of phones. Different versions of the PDS will be available for enterprise customers and service providers.

A limited version of PDS functionality can be observed in the pingtel.net calling service. When this personal calling service is used, it supplies configuration data to designated xpressa phones automatically. See page 104.

Note Until the release of the Pingtel Deployment Server, you configure xpressa phones one at a time. See Configuring an xpressa phone on page 24.
Introduction

Support services

Documentation resources
Pingtel provides guides with detailed information on the xpressa phone, instant xpressa softphone, and xDK. Find these and other publications on Pingtel's web site at http://www.pingtel.com/docs.

For phone users
Using Pingtel phones provides information to help you use an xpressa phone. An appendix describes the instant xpressa softphone.

For third party programmers
The xDK Guidelines for User Interface Design defines characteristics of a consistent, easy to use xpression application and recommendations for designing its user interface.

The xpressa Development Kit Programmer’s Guide describes the xDK, which provides tools for developers of Java applications for Pingtel xpressa phones.

The xDK Programmer’s Reference Manual details Pingtel's published APIs for developing applications for xpressa phones.

All guides are optimized for online review. Click on any cross reference, such as a page number, to go directly to that page. For best results when printing use Acrobat Reader’s Fit to page or Expand small pages option.

Using www.pingtel.com
Visit Pingtel's web site at http://support.pingtel.com/ for detailed information about Pingtel's support services, the latest software downloads and upgrades, troubleshooting tips, information on logging product defects, and all product documentation.
If you have a question, you can also send e-mail to support@pingtel.com.

**Contacting Pingtel**

For response from Pingtel’s Technical Assistance Center (TAC), use the web site resources described above or send your questions by e-mail to support@pingtel.com. To contact the TAC by phone:

- From within the US, call toll free 1-800-PINGTEL (1-800-746-4835).
- From outside the US, call (781) 938-5306.

When you send e-mail or before you call, record the hardware model number, serial number (MAC address), and REV manufacturing code that appear on the label on the bottom of the xpressa phone. This information may be required to help resolve your problem.

**Tip** You may be able to resolve the problem yourself: please review the section on *Troubleshooting* on page 119.
Installing an xpressa phone

Install a xpressa phone

Pingtel ships xpressa phones with the following components:

- An xpressa phone base with attached phone foot
- A phone handset with cord
- A Cat 5 network cable

These additional components are included on request:

- A Power Insertion Module (PIM)
- A power transformer with power cord

Tip: To supply power at local standard voltage, Pingtel ships a power transformer that is appropriate for an xpressa phone’s destination country.
Initial assembly

Use the connection jacks on the phone's base to connect the handset and any optional equipment to the xpressa phone’s base. See Setting up your xpressa phone in Using Pingtel phones for additional detail on these tasks. Then determine the power source for the xpressa phone.

xpressa phone power sources

You provide Inline Power to an xpressa phone by connecting a single Cat 5 network cable to it. To supply power to this cable, you can use either power from a wall outlet or power from a Cisco® switch or Inline Power patch panel supporting Inline Power. Descriptions of these options follow.

Tip The xpressa phone is not compatible with equipment that is 100 Base-T only. Your hub or switch must be 10 Base-T or 10/100 to be compatible.

To maintain power in the event of a power outage, use of an uninterruptible power supply (UPS) is recommended for LAN hubs and switches, WAN access equipment, and the xpressa phone.

Wall outlet

Power from a wall outlet is supplied by the power transformer to the Power Insertion Module (PIM) and from the PIM to the xpressa phone. To use this power source, you employ the supplied network cable, the power transformer, and the PIM. You must also supply one additional Cat 5 cable. The network cables connect the xpressa phone to the PIM and the PIM to a 10 Base-T Ethernet/LAN.

Caution

When you connect the Cat 5 network cable to the PIM, the cable carries approximately 24 volts of power on pins 4 and 5 (negative polarity) and 7 and 8 (positive). Connect this cable only to an xpressa phone and not to any other equipment.
Installing an xpressa phone

Cisco® switch or Inline Power patch panel

To supply power from a Cisco® switch or Inline Power patch panel supporting Inline Power to the xpressa phone, you use the supplied Cat 5 cable to connect the xpressa phone to the 10 Base-T or 10/100 Ethernet/LAN. Cisco’s Inline Power equipment automatically detects whether to connect a device only to the network or to both power and the network.

The power transformer and PIM are not used if the phone receives power from a Cisco® switch or Inline Power patch panel supporting Inline Power.

Installing with power from the PIM

You supply one additional Cat 5 cable for this powering option.

1. Use the supplied network cable to connect the phone to the PIM-1. This cable connects to the side of the PIM-1 that has only one connection. The Cat 5 network cable you connect to the phone must have all four pairs of wires; cables with only two pairs of wires do not provide a complete connection.

2. Connect the additional network cable to the side of the PIM-1 that has both network and power connections, then connect that cable to your 10 Base-T or 10/100 Ethernet/LAN port.

3. Connect the power transformer to the PIM-1, then plug in the power transformer. The xpressa phone starts as described on page 16.
To connect both a PC and the xpressa phone to the network when only one network port is available, connect both the PC and the PIM to an Ethernet hub or switch, then connect the hub to the network port as illustrated here:

**Installing with Inline Power**

This option provides power to the xpressa phone from a Cisco switch or Inline Power patch panel that supports Inline Power. This powering option does not use the power transformer or the PIM.

1. Connect the supplied network cable to your 10 Base-T or 10/100 Ethernet/LAN port.
2. Connect the network cable to the xpressa phone.
Installing an xpressa phone

The xpressa phone starts as described on page 16.

**Tip** If only one network port is available and you need to connect both the xpressa phone and a PC to the network, follow the instructions for *Installing with power from the PIM* on page 14 and use an Ethernet hub or switch.

**xpressa phone startup**

As soon as an xpressa phone receives power, it starts. By default, the xpressa phone will immediately attempt to contact a DHCP (Dynamic Host Configuration Protocol) server on your Ethernet/LAN.

- If a DHCP server is available, the xpressa phone obtains a DHCP lease with network settings, including an IP address.
- If your network does not have a DHCP server, and you have not yet defined static network values for the phone, startup may take several minutes while the DHCP requests time out.
- If you choose to define static network settings for the phone, those values are used at start up instead of dynamic addresses supplied by a DHCP server. See *Setting static network values* on page 20.

**Tip** A phone may take a long time to determine that your network does not have a DHCP server or that a supplied static address is invalid. If startup takes a long time, try connecting the phone to power only. With no network connection, the xpressa phone starts more quickly so that you can verify or supply static network values as described on page 20.
When its network settings are confirmed, the xpressa phone displays a splash screen and plays a startup audio file.

You can adjust the phone’s contrast and volume settings when startup is complete.

**Tip** When a new software release is available, an additional prompt displays during startup. See page 108.

The xpressa phone loads software and configuration data next. When all installed xpression applications load, startup is complete. The xpressa home screen displays.

You can restart xpressa phones at any time. See page 113.
Assigning network settings

To function as part of your Ethernet/LAN, an IP address, net mask, gateway, and DNS server must be assigned to each xpressa phone. This section describes how you can:

• Use dynamic (DHCP) network settings for xpressa phones.
• Set static network values on xpressa phones.

Network settings must be assigned to an xpressa phone through one of these methods before it can be used to make and receive calls.

Optional network settings are also available for xpressa phones:

<table>
<thead>
<tr>
<th>For information on</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying a time server</td>
<td>page 61</td>
</tr>
<tr>
<td>Including 802.1p signaling in VLAN QoS headers</td>
<td>page 102</td>
</tr>
<tr>
<td>Specifying the Ethernet duplex mode</td>
<td>page 69</td>
</tr>
</tbody>
</table>

To assign or change network settings you must supply the admin user name and password. See Administrative log on on page 39.

Dynamic (DHCP) network settings

If your Ethernet/LAN includes a DHCP (Dynamic Host Configuration Protocol) server, each installed xpressa phone uses DHCP by default to supply its network settings automatically.

• If an xpressa phone finds a DHCP server you do not need to provide static network settings.
• If your network does not have a DHCP server, or if you prefer not to use dynamic addressing, you must define static values for the network settings. See page 20.
If you plan to use DHCP to provide network addresses, but your DHCP server does not supply the address of a DNS (Domain Name System) server, you can manually specify a primary and secondary DNS address for the xpressa phone to use.

**Identifying a DNS server**

Most DHCP environments supply a DNS server address. However, if your DHCP environment does not return a DNS address, you can supply primary and secondary DNS server addresses for the xpressa phone to use. The xpressa phone uses a DNS server to locate such network resources as SIP servers and xpression applications.

**Note** The xpressa phone only uses the DNS servers at these addresses if DHCP does not supply a server address.

To supply the address of a DNS server:

1. From the xpressa phone's home screen, press **MORE**.
2. On the Apps tab, press **Prefs**.
   You may need to scroll down to find Prefs on this tab.
3. Select the Network Settings category then press **Adjust**.
   This task requires the administrative password. See page 38.
4. On the Network Settings screen, verify that Use DHCP is selected.
Assigning network settings

5 Select the Primary DNS field, then enter the DNS server’s address. This is a numeric entry field. Press * to insert a separator; for example, enter 100*10*10*130 for an address of 100.10.10.130. Correct mistakes with the Backspace and Move Left or Move Right commands.

6 Optionally, scroll down and select Secondary DNS to enter another DNS address.

7 Press OK and then restart the xpressa phone. Your new setting does not take effect until you restart the phone.

Tip You can also specify the address of a time server (see page 61) or include 802.1p signaling in VLAN QoS headers (see page 102).

Static network settings

To provide a set of static network values for an xpressa phone, determine and record the values for:

- IP address
- Net mask
- Gateway
- Primary DNS server
- Secondary DNS server (optional)

Setting static network values

You set static network values directly on an installed xpressa phone using the phonetop interface.

1 From the xpressa phone’s home screen, press MORE.

2 On the Apps tab, press Prefs. Scroll down if necessary to find this xpression application.
3 Select the Network Settings category then press Adjust. This task requires the administrative password. See page 38.
4 Press the Supply Static radio button. Scroll down to review the data entry fields added to this screen.

5 Select the IP address field, then enter the xpressa phone’s IP address. This is a numeric entry field. For a . separator press *. Correct mistakes with the Backspace, Move Left, and Move Right commands.
6 Repeat step 5 to enter values for:
   - Network mask
   - Gateway
   - Primary DNS address

7 Optionally, select Secondary DNS and enter another DNS address.
Assigning network settings

8 Press OK and then restart the xpressa phone.
       Your new settings do not take effect until you restart the phone.

Tip You can also use the Network Settings preference category to specify the
       address of a time server (see page 61) or include 802.1p signaling in VLAN
       QoS headers (see page 102).

Verifying network settings

To review the network settings of an xpressa phone, start the Prefs xpres-
       sion and choose the Network Settings category as described on page 20.
In addition, any user can verify the IP address assigned to a phone without
       providing the administrative password:
1 From the xpressa home screen, press MORE.
2 On the Menu tab press About.
3 Press Info.
       Information about the xpressa phone displays, including its IP address.
4 Press OK to return to the xpressa home screen.
Switching from static to DHCP

You can modify an xpressa phone’s network configuration to use values provided by a DHCP server instead of previously entered static values.

1. Start the Preferences xpression: from the xpressa phone’s home screen, press MORE, then on the Apps tab choose Prefs.
2. Select the Network Settings category and press Adjust.
   This task requires the administrative password. See page 38.
3. Press the Use DHCP radio button.
4. Press OK then restart the xpressa phone.

Your new settings do not take effect until you restart the phone.
Configuring an xpressa phone

In addition to the network settings that an xpressa phone uses, you define values for configuration parameters. These parameters control the operation of an xpressa phone. The xpressa phone stores its configuration data in two ASCII text files: `pinger-config` and `user-config`. You change the default values supplied in these files to suit the requirements of your installation and the phone's current user.

This section describes the interfaces for configuring xpressa phones and the default configuration values supplied with every xpressa phone.

- For descriptions of the specific parameters that you use to configure phones, start on page 46.
- For a quick reference to every configuration parameter, see Appendix B: Parameter reference on page 160.

Tip Before you configure an xpressa phone, its network settings must be defined. See page 18.

Configuration interfaces

To add or change configuration values you use:

- The phonetop interface of a specific xpressa phone.
- A PC to access the browser-based interface of any xpressa phone in the same network, or the MyPingtel user portal.

You can also edit the `pinger-config` and `user-config` ASCII text files on your PC, then upload them to a phone using the browser-based interface.

Tip Parameters can be set on the phonetop, with the browser-based interface, or using both interfaces.
Using the phonetop interface

The phonetop interface allows you to set values for configuration parameters directly on a specific xpressa phone.

- This interface requires physical access to a specific xpressa phone. As a result, the phonetop interface is best suited to controlling features that apply to a specific phone or user, such as parameters for handling incoming calls or controlling the phone’s embedded web server.
- You can only access a subset of the parameters with this interface. Appendix B: Parameter reference on page 160 provides a quick way to determine whether or not you can set a parameter with this interface.

For complete information on the xpressa phone’s user interface, see User interface fundamentals in Using Pingtel phones.

1. From the xpressa phone’s home screen, press MORE.
2. On the Apps tab press Prefs. You may need to scroll down to find Prefs on this screen.

3. Select a preference category:

<table>
<thead>
<tr>
<th>Select</th>
<th>To set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Settings</td>
<td>Network addresses and values. See page 20. Also used to specify a time server or the use of VLAN QoS signaling.</td>
</tr>
<tr>
<td>Call Handling</td>
<td>Parameters for managing incoming calls. See page 55.</td>
</tr>
</tbody>
</table>
Configuring an xpressa phone

<table>
<thead>
<tr>
<th>Select</th>
<th>To set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time &amp; Locale</td>
<td>Parameters for keeping local time. See page 61.</td>
</tr>
<tr>
<td>Volume &amp; Contrast</td>
<td>Volume and contrast levels. See Customizing your xpressa phone in Using Pingtel phones.</td>
</tr>
<tr>
<td>myxpressa Web</td>
<td>Access to the xpressa phone's browser-based interface. See page 63.</td>
</tr>
<tr>
<td>User Maintenance</td>
<td>Administrative security. See page 41.</td>
</tr>
</tbody>
</table>

All users can access the Call Handling, Time & Locale, and Volume & Contrast categories. However, Network Settings, myxpressa Web, and User Maintenance require you to log in as the admin user. See page 39.

4 Press Adjust.
5 Use the data entry controls provided to add and change configuration values.

Tip Using Pingtel phones provides additional detail on setting values on the phonetop.

Using the browser-based interface

The browser-based interface provides access from any PC to any xpressa phone that has its embedded web server enabled. This interface provides broader access to parameter settings than the phonetop interface.

Tip The exception is the parameter that enables and disables web access to the xpressa phone. If web access to an xpressa phone is disabled, you can only reenable it through the phonetop interface: in Prefs, choose the myxpressa Web category. For more information on the PHONESET_HTTP_PORT parameter see page 63.

1 On a PC, open a web browser.
2 In the browser’s Address or Location field, enter the xpressa phone’s
IP address and optionally the HTTP port.
For example, enter http://10.20.30.40:8080
The port number is required only if you provide a value other than 80 for the PHONESET_HTTP_PORT parameter. See page 63.

3 Enter admin as the user name and your administrative password in the dialog box that opens.
Initially, the password is not defined: don’t enter anything in the password field. For more information see page 38.
The myxpressa home page opens.
Configuring an xpressa phone

4a To set Call Handling or Time & Locale parameters, click Preferences: Preferences.
4b To set other parameters, click Administration: Phone Configuration.
   A web page opens with configuration options.
5 Follow the instructions on this page to add and edit values.
   Detailed descriptions of each parameter begin on page 46.
6 Click Save.
7 Click Restart to restart the xpressa phone.
   New values do not take effect until you restart the phone.

Using the MyPingtel user portal

With the MyPingtel user portal, users can set values for a limited number of parameters from the web browser of any PC. To use MyPingtel, the xpressa phone must have its embedded web server enabled and a user must register him- or herself and one or more phones to use the site.

This guide notes the parameters that can be set from MyPingtel. For information on registering for and using MyPingtel, visit http://my.pingtel.com or see MyPingtel user portal in Using Pingtel phones.

Configuration files

At startup, each xpressa phone searches its flash file system for both the pinger-config and user-config configuration files. If either file is not present, the xpressa phone creates that file with default configuration data automatically.

• In addition to using the phonetop and browser-based interfaces to set values, you can manually edit these configuration files.
• You can revert to default configuration data if necessary. See page 115.
Editing configuration files manually

To employ this configuration method, you use a browser to download a phone’s configuration files, edit the files with an ASCII text editor, then use the browser to upload the edited files to the phone. This process can be useful when you want several phones to have similar configurations, or if you need to configure several phones in a short period of time.

This section describes formatting requirements, exceptions, and the procedures you use to edit \texttt{user-config} and \texttt{pinger-config} effectively.

Tip The parameters and values you add to the \texttt{user-config} file override values in the \texttt{pinger-config} file.

Parameter name : value format

When you add a parameter and value to the \texttt{pinger-config} or \texttt{user-config} file the spacing and punctuation that you use are important. Enter the complete parameter name, a space, a colon, another space, and then the value. For example:

\texttt{PHONESET_BUSY_BEHAVIOR : BUSY}

Tip When you use the xpressa phone’s browser-based interface you enter only the value. You do not enter the parameter name.

Value format

For some parameters, you must use a specific format when you supply a value. For example, when you enter the address of a SIP server be sure to use the format \texttt{sip:<fully qualified host name>}. This guide supplies specific formatting information as applicable with the description of each parameter.
Configuring an xpressa phone

Parameters with specific valid values

For other parameters, you must supply one of a specific set of valid values. For example, BUSY or FORWARD are the only valid values for the PHONESET_BUSY_BEHAVIOR parameter.

- When you set a value for one of these parameters with the browser-based interface or on the phonetop, a data entry control such as a check box or a drop down list assures that you provide a valid value.

- When you manually edit the pinger-config or user-config file, be sure to supply only a valid value. This guide lists the valid values for parameters that have this requirement.

If you enter an invalid value in pinger-config or user-config, the xpressa phone uses the default value for that parameter.

Parameters that store multiple values

For most configuration parameters you store only one value. Some parameters, however, can be added to a configuration file more than once, to store data for use in different situations. A dot or period appears at the end of the names of these parameters. For example:

PHONESET_DIGITMAP. :
SIP_AUTHORIZE_USER. :

You then supply two different values for these parameters: one identifies the specific use of the parameter and becomes part of the name, while the other is its corresponding value. For example, when you set up a digit map you place the specific dial plan after the dot, and the SIP address to use for that dial plan after the colon:

PHONESET_DIGITMAP.0 : sip:operator@mycompany.com
PHONESET_DIGITMAP.911 : sip:911@215.133.0.14
You set up authorized users for outgoing calls with the same format: the SIP URL of the destination that requires authentication comes first, then the assigned, authorized user name:

SIP_AUTHORIZE_USER.tparker@sopark.com : tparker  
SIP_AUTHORIZE_USER.rsmith@cure.com : robert

For more information on digit maps see page 48. For more information on authenticating outgoing calls see page 89.

**Note** For the PHONESET_SNMP_TRAP_DESTS parameter you can specify up to eight values. You enter them all on one line separated by spaces.

**Exceptions**

You can set most parameters by manually editing **pinger-config** or **user-config** in this way. There are two exceptions:

- Use the phonetop interface to set the PHONESET_HTTP_PORT parameter. This parameter enables and disables web access to an xpressa phone.
- Use the browser-based interface to set user names and passwords. The browser-based interface automatically encrypts the password when it stores these values for the PHONESET_HTTP_AUTH_DB parameter. Use either the browser-based interface or the phonetop to change the password for the admin user.

**To edit a configuration file**

1. On the myxpressa home page, click **Administration: File Uploads**. For information on accessing the myxpressa home page, see page 26.
2. Enter admin and the administrative password. A web page for installing and reviewing software files opens.
Configuring an xpressa phone

3a To edit the pinger-config file, under **Phone configuration** click View current configuration.

3b To edit the user-config file, under **User configuration** click View current configuration.
Configuration files

The selected configuration file displays in your browser.

4 From the File menu select **Save As** and save pinger-config or user-config in a plain text (.txt) file on your local PC.

5 Open the saved pinger-config.txt or user-config.txt file in an editor such as Notepad.

6 Edit the values for the parameters you wish to change, or add parameters and values as required. Save your edits.

7 Use your browser’s Back feature to return to the File Uploads page.

8 In the Phone configuration section, browse for and enter the name of your edited pinger-config.txt file.

   Alternatively, in the User configuration section browse for and enter the name of your edited user-config.txt file.
Configuring an xpressa phone

9 Click the **Upload** button for the file.
   Your newly defined parameters load into the xpressa's flash file system.

10 Click **Restart** to restart the xpressa phone.

**To edit files for instant xpressa**

For an instant xpressa softphone, the configuration files are located in the pingtel\instantXpressa\env directory. You do not need to use the browser-based interface to access or upload these files: instead, use Windows Explorer to locate a configuration file, open the file in an editor, then save your edits and restart instant xpressa.

**To configure multiple phones**

If you edit a configuration file manually, you can configure several phones quickly: after downloading and editing a file for the first phone and uploading it, proceed by editing the same file again to specify unique values such as an extension number for a second phone, then upload it to that phone. Repeat as needed for additional phones.

**Reviewing configuration files**

1 On the myxpressa home page, click **Administration: File Listing**.
   For information on accessing the myxpressa home page see page 26.
   A list of files stored on the xpressa phone opens.

2 To review the pinger-config file click **pinger-config**; to review the user-config file click **user-config**.
   The contents of this file display in your browser.

   Alternatively, you can follow step 1 through step 3b on page 31 to review configuration files.

**Tip** For instant xpressa, find these files in pingtel\instantXpressa\env. Open these files in an editor such as Notepad.
Default pinger-config file

By default, the pinger-config file of an xpressa phone contains:

```plaintext
PHONESET_AVAILABLE_BEHAVIOR : RING
PHONESET_BUSY_BEHAVIOR : BUSY
PHONESET_CALL_WAITING_BEHAVIOR : ALERT
PHONESET_DIALPLAN_LENGTH : 4
PHONESET_DND_METHOD : FORWARD_ON_BUSY
PHONESET_EXTENSION : 4444
PHONESET_HTTP_PORT : 80
PHONESET_RINGER : BOTH
PHONESET_RTP_PORT_START : 8766
PHONESET_TIME_DST_RULE :
PHONESET_TIME_OFFSET :
PHONESET_TIME_SERVER :
SIP_AUTHENTICATE_REALM :
SIP_AUTHENTICATE_SCHEME :
SIP_DIRECTORY_SERVERS :
SIP_FORWARD_ON_BUSY :
SIP_FORWARD_ON_NO_ANSWER :
SIP_FORWARD_UNCONDITIONAL :
SIP_PROXY_SERVERS :
SIP_REGISTER_PERIOD : 3600
SIP_REGISTRY_SERVERS :
SIP_SESSION_REINVITE_TIMER :
SIP_TCP_PORT : 5060
SIP_UDP_PORT : 5060
```

After you configure an xpressa phone its pinger-config file contains additional parameters and values. See Appendix B: Parameter reference on page 160 for a list of all parameters with their defaults and sample values.

Default user-config file

By default, the user-config file for an xpressa phone contains these parameters, including the admin user name and its default, encrypted password:
Configuring an xpressa phone

PHONESET_TIME_SERVER :
PHONESET_HTTP_AUTH_DB.admin : cc3779c1114ba5fd9882afdc7ef267e3

After user preferences are set for an xpressa phone, its user-config file contains additional parameters and values.

See Using administrative security features on page 38 for more information on this parameter.

Using the browser-based interface

If you make changes to an xpressa phone’s configuration with the browser-based interface, the parameters are automatically redistributed among the pinger-config and user-config files.

The browser-based interface saves these parameters in pinger-config:

PHONESET_ADMIN_DOMAIN
PHONESET_DEPLOYMENT_SERVER
PHONESET_DIALPLAN_LENGTH
PHONESET_EXTENSION
PHONESET_EXTERNAL_IP_ADDRESS
PHONESET_LOGICAL_ID
PHONESET_RTP_PORT_START
SIP_AUTHORIZE_PASSWORD
SIP_AUTHORIZE_USER
SIP_DIRECTORY_SERVERS
SIP_PROXY_SERVERS
SIP_REGISTER_PERIOD
SIP_REGISTRY_SERVERS
SIP_SESSION_REINVITE_TIMER
SIP_TCP_PORT
SIP_UDP_PORT

The browser-based interface saves these parameters in user-config:

ALLOW_CONSOLE_OUTPUT
JAVA_OUTPUTSTREAM_REDIRECT
PHONESET_AVAILABLE_BEHAVIOR
PHONESET_BUSY_BEHAVIOR
Tip Values in the user-config file override values in the pinger-config file.
Using administrative security features

To prevent unauthorized access to xpressa phones, all xpressa phones come with an administrative user name and password.
- The user name is *admin* (case sensitive).
  You cannot change the *admin* user name.
- Initially, no password is set.
  To customize this security feature you can change the *admin* password: see page 41.

You must log on as *admin* to perform a protected task with either the phonetop or browser-based interface. In addition, the browser-based interface always requires a user name and password. Log on as *admin* to perform all tasks, or set up individual authorized users to access non-protected tasks through this interface. See page 44.

**Note** You also use the *admin* log on for Telnet access to xpressa phones. For information on enabling Telnet access, see page 55. Telnet should only be used under the direction of Pingtel's Technical Assistance Center (TAC).

Protected tasks

You supply the administrative user name and password to access a protected task through either the phonetop or the browser-based interface.

**On the phonetop**

On the xpressa phonetop, you access protected tasks through the Prefs xpression. You must supply the administrative password when you select these preference categories:
- Network settings
  For more information see page 18.
myxpressa Web
Enables or disables access to the phone’s browser-based interface. See page 64.

User maintenance
Changes the administrative password. See page 41.

**With the browser-based interface**
When you work with the browser-based interface, only a user who logs on as **admin** can select these Administration options:

- **User Maintenance**
  Allows you to set up user names and passwords. See page 44.

- **Phone configuration**
  Provides the browser-based interface for working with phone configuration values. See page 26.

- **File Uploads**
  Allows you to upload files to an xpressa phone, including configuration files (see page 29) and software upgrades (see page 107).

- **Upgrade Log**
  Records software upgrades. See page 142.

- **File Listing**
  Provides file names and sizes. See page 143.

**Administrative log on**
After you select a password-protected option, you are prompted to supply the administrative password. You do not need to supply the password again while you continue to work in Prefs, or until you exit from your browser.
Using administrative security features

Logging on to the phonetop

1. Enter the defined administrative password.
   Initially, no password is set. You can define an alphanumeric password:
   press each dial pad button once, twice, or more to enter the password
   correctly.

2. Press OK.
   Alternatively, press Cancel for read-only access.

See User interface fundamentals in Using Pingtel phones for information
on entering alphanumeric data on the phonetop.

Logging on to the browser-based interface

1. In an HTML browser’s Address or Location field, enter the phone’s
   IP address and optionally the HTTP port as described on page 64.
   A dialog box opens.

2. Enter the administrative user name: admin

3. Enter the defined administrative password.
   Initially, no password is set.

4. Click OK.
Change the administrative password

You can change the administrative password at any time. If the security standards of your organization require you to set an administrative password for the xpressa phones, Pingtel recommends that you define a single password and then set that password on every xpressa phone. You must set the password on each phone individually.

A password can consist of upper- and lower-case letters, digits, and symbols.

Tip The user name admin cannot be changed.

Changing the password on the phonetop

1. From the xpressa phone’s home screen, press MORE.
2. On the Apps tab press Prefs.
   You may need to scroll down to find Prefs on this tab.
3. Select the User Maintenance category then press Adjust.
4. Enter the current administrative password: since a password can be alphanumeric, you may need to press the dial pad buttons more than once to enter each character.
5. Press OK.
   Initially, no password is set: simply press OK.
6. Select the Change admin password option then press Adjust.
Using administrative security features

7 Use the dial pad to enter the New password. This is an alphanumeric field. Press each dial pad button once or more to access each of the letters and the number that are assigned to it.

8 Press OK.
   A password verification screen displays.

9 Re-enter the password to confirm it then press OK.

See User interface fundamentals in Using Pingtel phones for information on entering alphanumeric data on the phonetop.

Changing the password with a browser

1 On a PC, open a web browser.

2 In the browser's Address or Location field, enter the phone's IP address and optionally the HTTP port. For example, http://10.1.1.123:8080
   The port number is required only if you set this myxpressa Web parameter to a value other than 80. See page 64.

3 Enter the user name admin and the current administrative password.
   The myxpressa home page opens.

4 Click Administration: Change Password.
   A web page for changing the current user’s password opens.
Reset the administrative password

5 Verify that the user name that displays is admin.
   You must log in as the administrator in order to change this password.

6 Enter a new password.

7 Re-enter the password to confirm it then click Change Password.

Tip Your browser may present an “Authorization failed” message. If so, enter the new password and click OK.

Reset the administrative password

If you cannot identify the correct administrative password for an xpressa phone, it is possible to set its password back to a null value. To do so, you
Using administrative security features

must reset the xpressa phone to its factory default settings. This action replaces all of the configuration settings for the phone, including the administrative password, with default values. For more information on reverting to factory defaults, see page 115.

Tip On an instant xpressa softphone, you can simply delete the parameter that stores the admin user name and password from the configuration file. For more information on working with configuration files see page 29.

Set up users for the browser-based interface

To protect an xpressa phone from unauthorized access, the browser-based interface always requires an authorized user name and password. Initially, you can only access the web interface of an xpressa phone using the admin user name and its password.

However, because the browser-based interface offers features for all users, including interfaces for call control, installing xpression applications, and setting up speed dial numbers, you may wish to authorize one or more users per phone to access the embedded web server through the browser-based interface.

Authorized users must be set up for each xpressa phone individually. Only a user who is authorized for a particular phone in this way can use its browser-based interface.

For each user that you set up, this procedure stores a value for the PHONESET_HTTP_AUTH_DB parameter.

Note If you establish a user name and password for the browser-based interface, it does not automatically provide access to the MyPingtel user portal. Users must register for MyPingtel separately and use the MyPingtel sign-in application. See MyPingtel user portal in Using Pingtel phones for more information.
Set up users for the browser-based interface

1. On the myxpressa home page, click **Administration: User Maintenance**.
   A web page for maintaining user data opens.
   For information on accessing the myxpressa home page see page 26.

2. In the Add User section of this form:
   - Enter the user name.
   - Enter a password.
   - Re-enter the password to confirm it.

3. Click **Add User**.
Basic configuration

This section describes the device-specific parameters that you set to define an xpressa phone’s behavior for:

- Dialing, including the phone’s identifying extension: see below.
- Security: see page 54.
- Incoming call handling: see page 55.
- Time settings: see page 61.
- Network management: see page 63.
- Home screen display: see page 70.

Set parameters for dialing

The configuration parameters for dialing define:

- A unique extension for each xpressa phone in your organization. This value should be supplied for an xpressa phone before it is used.
- Dial plan length to help automate dialing.
- Digit maps to help automate call addressing and dialing.

To set values for these parameters use the browser-based interface described on page 26.

Assigning a unique extension

PHONESET_EXTENSION

This parameter stores a value that uniquely identifies each xpressa phone to the SIP Registry server. This value can be a number or an alphanumeric identifier. By default, this parameter is set to 4444 on every xpressa phone.

For information on SIP Registry servers, see page 72.
Set parameters for dialing

You set the extension value with the browser-based interface described on page 26. Once set, the extension displays:

- In the title bar of the xpressa home screen. The extension alternates with the current date and time.
- On the ready screen, when the user lifts the handset or otherwise prepares to make a call.

Tip In some cases, you may want to assign the same extension to more than one xpressa phone. For example, in a system that uses a forking SIP proxy, you could assign the same extension to two phones so that when that extension value is dialed, both phones ring.

Automating dialing

PHONESET_DIALPLAN_LENGTH

With this feature you specify the length of the phone numbers that will be dialed most often from this xpressa phone. When a user dials, the xpressa phone detects when this number of digits has been entered and after a short pause sends the call invitation automatically. The user doesn’t need to press Dial to indicate that the number is complete.

For example, if an xpressa phone is used mostly to dial three-digit internal extension numbers, use the browser-based interface to set this parameter to 3. If North American long distance numbers are dialed, set it to 11.

By default, this parameter is set to 4. The length must be 2 or greater.

Tip PHONESET_DIALPLAN_LENGTH does not define a maximum or minimum length for dialing. However, when users dial a number that is shorter or longer, they must press Dial or # to indicate that the number is complete.
Basic configuration

The PHONESET_DIGITMAP parameter provides additional flexibility. If defined PHONESET_DIGITMAP value(s) override the value for this parameter.

Defining digit maps

PHONESET_DIGITMAP

The PHONESET_DIGITMAP parameter maps two values: a dial plan for a valid phone number type, and the SIP address to which phone numbers of that type should be routed. This parameter provides flexibility for installations that use different SIP addresses or servers for calls made to internal and external numbers, or for local and long distance numbers. You can also use this parameter to identify multiple acceptable phone number lengths and formats to automate dialing.

Defining the dial plan

A dial plan establishes the expected length and format of a typical, valid telephone number. When a user dials a number that has the same length and format as a predefined dial plan, the xpressa phone can recognize that dialing pattern and route it to the appropriate SIP address automatically when it is complete.

In the US, some typical dial plans include:

- Internal extension numbers of two, three, or four digits.
- Local numbers of seven digits, which may be preceded by a 9 if required to access an outside line.
- Long distance numbers of eleven digits, consisting of a 1, then a three-digit area code, then a seven-digit number. These also may be preceded by a 9 if required.
Dial plan syntax

The syntax used to identify dial plans is adapted from IETF Request for Comments 2705, section 2.1.5.

<table>
<thead>
<tr>
<th>To specify a</th>
<th>Enter</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digit</td>
<td>0 1 2 3 4 5 6 7 8 9 *</td>
<td>Identifies a specific digit.</td>
</tr>
<tr>
<td>Range</td>
<td>[digit-digit] [digit-digit, digit]</td>
<td>Identifies any digit dialed that is included in the specified range or as a comma-separated individual digit.</td>
</tr>
<tr>
<td></td>
<td>For example, if a range of [0-1, 8-9] is a part of the dial plan, a dialed number that includes 0, 1, 8, or 9 in that position will match.</td>
<td></td>
</tr>
<tr>
<td>Wildcard</td>
<td>x</td>
<td>x matches any single digit that is dialed.</td>
</tr>
<tr>
<td></td>
<td>.</td>
<td>. matches an arbitrary number of digits, including none.</td>
</tr>
<tr>
<td>Timer</td>
<td>T</td>
<td>Indicates that an additional time out period, totalling four seconds, should take place before automatic dialing begins.</td>
</tr>
<tr>
<td></td>
<td>Only one timer can be included per dial plan, and it must be the last character in the dial plan.</td>
<td></td>
</tr>
</tbody>
</table>

The # character should not be used in dial plans. The xpressa phone reserves # for users to indicate that dialing is complete.
Some examples of the syntax to use for different dial plans in a SIP phone environment follow:

<table>
<thead>
<tr>
<th>For calls to</th>
<th>Users dial</th>
<th>Set up dial plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal extension</td>
<td>a two-digit number</td>
<td>xx</td>
</tr>
<tr>
<td>Local number</td>
<td>9 (if required for an outside line) and then a seven-digit number. 9xxxxxxxT or xxxxxxxT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The timer assures that dialing is complete after this set of digits and that this is not, for example, a long distance number.</td>
<td></td>
</tr>
<tr>
<td>Emergency</td>
<td>911</td>
<td>911</td>
</tr>
<tr>
<td>Local operator</td>
<td>9 (if required for an outside line) then 0. 90T or 0T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The timer assures that the user has stopped dialing after these two digits and that this is not, for example, an internal extension.</td>
<td></td>
</tr>
<tr>
<td>Long distance number</td>
<td>9 (if required), 1, a three-digit area code, and then a seven-digit number 91xxxxxxxxx or 1xxxxxxxxx</td>
<td></td>
</tr>
<tr>
<td>International number</td>
<td>9 (if required), 011, and then any number of additional digits. The timer provides assurance that the number is complete before automated dialing begins. 9011x.T or 011x.T</td>
<td></td>
</tr>
</tbody>
</table>

Setting up a dial plan

On the web page for entering configuration values you specify the dial plan first, before a separating space and colon. For example:
If you edit the **user-config** file directly, you enter the dial plan after the parameter name and a period (.) as follows:

```plaintext
PHONESET_DIGITMAP.9xxxxxxxT :
```

You supply the SIP address that corresponds to this dial plan after the colon. See below for more information on supplying a SIP address.

You can enter each of the dial plans for your PHONESET_DIGITMAP configuration parameter on an individual line, or you can concatenate several dial plans together into a single string. To do so, you separate each dial plan with a vertical bar or “pipe” character (|), and enclose the complete string in parentheses.

For example, this single string describes the example dial plans shown on page 50:

```plaintext
(xx|9xxxxxxxT|911|90|91xxxxxxxxxx|9011x.T) :
```

However, all of the dial plans in a concatenated string map to the same SIP address. To map dialing plans to different SIP addresses, you can set them up individually, or set up different concatenated subsets like this:

```plaintext
(xx|9xxxxxxxT) :
(911) :
(90|91xxxxxxxxxx|9011x.T) :
```
Basic configuration

Where each subset will map to a different SIP address.

The next section describes setting up SIP addresses for dial plans.

Tip Set the PHONESET_DIALPLAN_LENGTH parameter to a value equal to the longest dial plan you define for the PHONESET_DIGITMAP parameter.

SIP addresses for digit maps

The address portion of a PHONESET_DIGITMAP value identifies a SIP Proxy server, SIP Redirect server, SIP gateway, or SIP phone. For example, these dial plans map to different SIP addresses:

In the user-config file you enter these values as:

PHONESET_DIGITMAP_0 : sip:operator@mycompany.com
PHONESET_DIGITMAP_411 : sip:helpdesk@mycompany.com
PHONESET_DIGITMAP_(911|9911) : sip:911@10.1.1.123
PHONESET_DIGITMAP_9xxxxxxT : sip:{digits}@localservice.net

Note If you set up a digit map for an emergency number, consider supplying the IP address of a gateway within your enterprise as the SIP address. This procedure minimizes reliance on a DNS server or SIP proxy in an emergency.
Supplying the SIP address portion of a digit map is optional: if you do not supply a specific SIP address for one or more of your defined dial plans, the xpressa phone uses the SIP server defined for the 
SIP_DIRECTORY_SERVERS parameter as the SIP address for all calls that match that dial plan.

For example, in an environment where the SIP Directory server has been set to sip:sip.pingtel.net, this sample digit map specifies the address of the SIP Directory server as the SIP address:

9xxxx : sip:{digits}@sip.pingtel.net

The same result is accomplished by the following definition:

9xxxx :

As this example shows, you have the option to supply the string {digits} as a part of any SIP address to represent the string of dialed digits. When a user dials a number that matches the dial plan, the dialed digits are substituted for this placeholder to establish the SIP address.

For example, with the browser-based interface you can set up digit maps as follows:

9xxxxxxxxT : sip:{digits}@localservice.net
91xxxxxxxxxx : sip:{digits}@longdistanceprovider.net

When a user dials to get an outside line and a local number, such as 9 375-4226, the call is addressed as:

dip:93754226@localprovider.net

To set up a digit map

To enter digit maps, use an individual line for each one. Enter the dial plan, a space, a colon (:), another space, and then the SIP address. Dial plans that use the same SIP address can be concatenated, as shown on page 51.
Basic configuration

Generally, you will need to set up a different PHONESETDIGITMAP value for each SIP address that is in use by your organization.

Secure xpressa phones

To prevent unauthorized changes to the xpressa phones in your installation, an administrative log on is supplied. You can also set up additional user names and passwords to control access via a phone's browser-based interface. The PHONESETHTTPAUTHDB parameter stores all user names and encrypted password values.

The PHONESETTELNETACCESS parameter controls your ability to Telnet to an xpressa phone. Telnet sessions require the admin user name and its defined password.

PHONESETHTTPAUTHDB

This parameter stores a user name and encrypted password to authorize access to certain functions on an xpressa phone. By default, this parameter is supplied with the user name admin and an encrypted password of null, as described on page 38.

PHONESETHTTPAUTHDB.admin : cc3779c1114ba5fd9882afdc7ef267e3

To change the admin password on the xpressa phone, start thePrefs xpression then select User Maintenance. To change this password with the browser-based interface, log in as admin and select Administration: Change Password.

To set up new users and their passwords, use the browser-based interface: select Administration: User Maintenance. As you set up additional users you save additional values for this parameter. See page 44 for more detail.

Tip

To give specific users access to multiple xpressa phones, set up the user names and passwords for those users on one phone using the browser-based interface. Then open the user-config file for that phone and copy
Set call handling parameters

the **PHONESET_HTTP_AUTH_DB** values (including the encrypted passwords) now stored in that file. For each of the other phones, paste the copied values into the **user-config** file and upload the edited file to each phone. See *Editing configuration files manually* on page 29.

**Note** The **PHONESET_HTTP_AUTH_DB** parameter also stores the user name and password for the MyPingtel user portal when a user registers the xpressa phone. The MyPingtel sign-in process also supplies values for parameters described on page 64.

**PHONESET_TELNET_ACCESS**

This parameter defines whether or not you can access an xpressa phone using Telnet. Options are ENABLE or DISABLE. By default, this parameter is set to DISABLE.

**Note** Initiate Telnet sessions only when directed to do so by Pingtel’s TAC. You change this value with the browser-based interface described on page 26. When set to ENABLE, this parameter allows you to Telnet to the xpressa phone from any PC in the network.

Telnet sessions require the **admin** user name and its defined password.

**Tip** The default **admin** password is not valid for Telnet access. You must define a specific **admin** password first.

**Set call handling parameters**

Call handling parameters determine how incoming calls will be handled by an individual xpressa phone by setting up:

- Alert method for incoming calls
- Call forwarding, with destinations for forwarded calls
- Call waiting
- Do not disturb, with direction for incoming calls
Basic configuration

Because end users may have different and changing needs for these settings, the administrative password is not required to define values for most call handling parameters.

Users can supply values for these parameters through:

- The browser-based interface: from the myxpressa home page, click Preferences.
- The phonetop interface: start the Prefs xpression then select Call Handling.
- The MyPingtel user portal: navigate to http://my.pingtel.com, log in, and from the myxpressa menu choose Call Handling.

The User interface fundamentals section in Using Pingtel phones describes use of the phonetop interface, browser-based interface, and MyPingtel user portal.

Selecting incoming call alerts

PHONESET_RINGER

This parameter determines how the user is alerted to an incoming call. Options are VISUAL, AUDIBLE, or BOTH. By default, this parameter is set to BOTH.

- VISUAL flashes the phone’s message waiting indicator.
- AUDIBLE plays the ring tone. Alternatively, if a call is in progress and PHONESET_CALL_WAITING_BEHAVIOR is set to ALERT, a call waiting beep plays.
- BOTH results in both alert types.

You can set alerts with either the browser-based or phonetop interface.
Setting up call forwarding

**PHONESET_AVAILABLE_BEHAVIOR**

This parameter defines what will happen when this xpressa phone receives an incoming call. Options are FORWARD, FORWARD_ON_NO_ANSWER, and RING. By default, this parameter is set to RING.

When this parameter is set to FORWARD, all calls are forwarded to the destination specified by the SIP_FORWARD_UNCONDITIONAL parameter.

If this parameter is not set to FORWARD all calls, the status of the xpressa phone, idle or busy, affects how incoming calls are handled:

- If the phone is idle when a call comes in, it will either RING or FORWARD_ON_NO_ANSWER, as set for this parameter. Use the SIP_FORWARD_ON_NO_ANSWER parameter to define the forwarding address.
  
  The PHONESET_NO-answer TIMEOUT parameter defines how long the phone must ring before it is considered to be unanswered.

- If the phone is busy when a call comes in, the phone uses the setting for the PHONESET_CALL_WAITING_BEHAVIOR parameter, or for the PHONESET_BUSY_BEHAVIOR parameter if call waiting is not enabled.

**SIP_FORWARD_UNCONDITIONAL**

Defines the address of another phone or voice mailbox: all incoming calls are redirected to this SIP URL or telephone number automatically. To enable this feature, you first set PHONESET_AVAILABLE_BEHAVIOR to FORWARD.

**SIP_FORWARD_ON_NO_ANSWER**

Defines the address of another phone or voice mailbox: incoming calls are redirected to this SIP URL or telephone number automatically if your phone
Basic configuration

Basic configuration is available; for example, you do not answer. To enable this feature, you set PHONESETAVAILABLE_BEHAVIOR to FORWARD_ON_NO_ANSWER.

PHONESETFNOANSERTIMEOUT
Defines the number of seconds that a phone must ring before it is considered to be unanswered or idle. By default, this parameter is set to 24; that is, after four rings of six seconds each.

**Tip** Enter a value that is a multiple of six for this parameter: 18, 24, 36, etc.

Defining call waiting or forward on busy

**PHONESETCALLWAITINGBEHAVIOR**
Determines whether or not call waiting is enabled when the phone is busy. Options are ALERT or BUSY.

- By default, this parameter is set to ALERT, which overrides any setting for the PHONESET_BUSY_BEHAVIOR parameter and enables call waiting.
- If BUSY, call waiting is disabled and the PHONESET_BUSY_BEHAVIOR value is used.

**PHONESET_BUSY_BEHAVIOR**
Defines what will happen when a call is placed to this xpressa phone and it is busy. To enable this parameter, PHONESET_CALL_WAITING_BEHAVIOR must be set to BUSY.

You can set the PHONESET_BUSY_BEHAVIOR parameter to BUSY or FORWARD. By default, this parameter is set to BUSY.

<table>
<thead>
<tr>
<th>Set to</th>
<th>Result when xpressa phone is busy</th>
</tr>
</thead>
<tbody>
<tr>
<td>BUSY</td>
<td>The caller hears a continuous busy signal.</td>
</tr>
<tr>
<td>FORWARD</td>
<td>Forwards any incoming calls to a previously defined destination. Use the SIP_FORWARD_ON_BUSY parameter to define the address of the forwarding destination.</td>
</tr>
</tbody>
</table>
Set call handling parameters

**SIP_FORWARD_ON_BUSY**
Defines the address of another phone or voice mailbox; incoming calls are redirected to this SIP URL or telephone number automatically if the xpressa phone is busy. To enable this feature, you first set PHONESET_BUSY_BEHAVIOR to FORWARD.

**Setting up Do Not Disturb**
Users can override all of their other call handling settings by enabling the Do Not Disturb feature. Do Not Disturb prevents the xpressa phone from giving any visual or audible alerts for incoming calls.

Two parameters control the Do Not Disturb feature: PHONESET_DND and PHONESET_DND_METHOD. All phone users can set the Do Not Disturb feature; however, only an administrator can set the handling method for incoming calls when Do Not Disturb is enabled.

**PHONESET_DND**
All users can set the PHONESET_DND parameter to ENABLE or DISABLE using the browser-based or phonetop interface or the MyPingtel user portal. When a user enables this feature, the xpressa phone does not provide notification for any incoming calls. Instead, incoming calls are handled as specified by the PHONESET_DND_METHOD.

By default, this parameter is set to DISABLE. When Do Not Disturb is enabled, this reminder icon displays on the xpressa home screen: 📣.

**Tip** When enabled, Do Not Disturb overrides all other call handling options.

**PHONESET_DND_METHOD**
Although any user can control when to enable or disable the Do Not Disturb feature, only administrators can set the PHONESET_DND_METHOD parameter to define how incoming calls will be handled when Do Not Disturb is enabled.
Basic configuration

You can set the `PHONESET_DND_METHOD` parameter to `SEND_BUSY`, `FORWARD_ON_BUSY`, or `FORWARD_ON_NO_ANSWER` through the browser-based interface. By default, this parameter is set to `FORWARD_ON_BUSY`.

<table>
<thead>
<tr>
<th>Set to</th>
<th>Result when <code>PHONESET_DND</code> = ENABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEND_BUSY</td>
<td>At the SIP messaging level, the xpressa phone sends a busy response to all call invitations. You can optionally configure a SIP server in your network to act on these messages and redirect “do not disturb” calls to another destination; otherwise, the caller hears a busy signal.</td>
</tr>
<tr>
<td>FORWARD_ON_BUSY</td>
<td>The xpressa phone responds to incoming calls as though it is busy. The caller either hears a busy signal or is forwarded if a destination has been specified as follows: <code>PHONESET_CALL_WAITING_BEHAVIOR = BUSY</code>, <code>PHONESET_BUSY_BEHAVIOR = FORWARD</code>, and <code>SIP_FORWARD_ON_BUSY = valid address</code>.</td>
</tr>
<tr>
<td>FORWARD_ON_NO_ANSWER</td>
<td>The xpressa phone responds to incoming calls as though there is no answer. The caller either hears ringing or is forwarded immediately if a destination has been specified as follows: <code>PHONESET_AVAILABLE_BEHAVIOR = FORWARD_ON_NO_ANSWER</code> and <code>SIP_FORWARD_ON_NO_ANSWER = a valid address</code>. Note that the <code>PHONESET_NO_ANSWER_TIMEOUT</code> is not applied.</td>
</tr>
</tbody>
</table>

The method you select for this parameter is invoked only when `PHONESET_DND` is set to ENABLE for the xpressa phone.
Define time-related parameters

The administrative password is required to set the PHONESET_DND_METHOD. You use only the browser-based interface to set this parameter.

Define time-related parameters

These parameters determine how time displays on an xpressa phone.

Specifying a time server

The administrative password is required to specify a time server to use in place of the default server. To define a time server using the phonetop interface, start the Prefs xpression then select the Network settings category. To define a time server with the browser-based interface select Administration: Phone Configuration.

PHONESET_TIME_SERVER

You can identify a host name or IP address for an xpressa phone to contact using SNTP (Simple Network Time Protocol) to obtain the correct time. If you do not add this parameter to your configuration file, the xpressa phone attempts to determine this value as follows:

• If the xpressa phone uses DHCP for network configuration and the DHCP NTP Server option is defined, that address is contacted.
• If you do not use DHCP for network configuration, or the DHCP NTP Server option is not defined, the xpressa phone attempts to contact one of a set of predefined, Internet-accessible time servers.

Setting the time to display

Any user can define the time zone and daylight saving time settings for a given xpressa phone. On the phonetop, start Prefs and choose Time & Locale; in a browser click on Preferences.
Basic configuration

**PHONESET_TIME_OFFSET**

This parameter defines the time offset from Coordinated Universal Time (UTC). Enter + or - followed by a value in minutes. If you do not specify a value for this parameter, the xpressa phone attempts to determine this value as follows:

- If the xpressa phone uses DHCP for network configuration and the DHCP Time Offset option is defined, that definition is used.
- If you do not use DHCP for network configuration, or the DHCP Time Offset option is not defined, the xpressa phone uses the time offset for the US Eastern time zone (-300 minutes).

**Tip** The phonetop interface allows you to choose a time zone; in the browser-based interface you define an offset value in minutes.

**PHONESET_TIME_DST_RULE**

This parameter determines the Daylight Saving Time (DST) rule for an xpressa phone to use. Options are NORTH_AMERICA, WESTERN_EUROPE, or NONE. Daylight saving time (DST) ends on the last Sunday in October. In Western Europe DST begins on the last Sunday in March; in North America DST begins on the first Sunday in April.

If you do not specify a value for this parameter, the xpressa phone uses the NORTH_AMERICA rule.

**Tip** The phonetop interface allows users to select either NONE or NORTH_AMERICA. Use the browser-based interface described on page 26 to choose any of the three options.
Set network management parameters

You can set configuration parameters to manage the xpressa phones in your network. You use network management parameters to:

- Enable and disable access to the phone via a web browser (below).
- Enable message waiting indication from a voice mail server (page 65).
- Send SNMP trap messages from the xpressa phone agent (page 67).
- Select the Ethernet duplex mode for the xpressa phone to use (page 69).

Additional parameters manage how xpressa phones work with firewalls, or define Quality of Service (QoS) settings. See page 94 for information on firewalls or page 101 for information on supporting QoS.

Controlling browser access

The value that you define for the PHONESET_HTTP_PORT parameter controls the ability to access an xpressa phone’s embedded web server through either its browser-based interface or the MyPingtel user portal. You can only define a value for this parameter by using the phonetop interface: start the Prefs xexpression then select the myxpressa Web category.

Access to the MyPingtel user portal also requires that values be set for:

- PHONESET_MYPINGTEL_PHONE_ID
- PHONESET_MYPINGTEL_SERVER
- PHONESET_MYPINGTEL_USERNAME

The user defines values for these parameters by using the MyPingtel Sign-In application to register the xpressa phone for the MyPingtel user portal. To change values for these parameters use MyPingtel Sign-In only.
Basic configuration

**PHONESET_HTTP_PORT**

This parameter identifies the port that the embedded web server should listen on. On an xpressa phone, this parameter is set to 80 by default.

If you disable the embedded web server, it does not run: the browser-based interface cannot be accessed and the MyPingtel user portal does not supply phone-specific data.

**Note** To prevent unauthorized access to a PC with the instant xpressa softphone installed, for instant xpressa softphones this parameter is disabled (set to 0) by default.

If you set the port number for this parameter to a value other than 80, such as 8080, to access the browser-based interface you must include that port number in the URL. The format is http://<ip address>:<port>.

**PHONESET_MYPINGTEL_PHONE_ID**

The MyPingtel user portal supplies a unique identifier to each phone when it is registered through the MyPingtel Sign-In xpression application. You can review this parameter in the user-config file. Running the MyPingtel Sign-In xpression sets the value for this parameter.

**PHONESET_MYPINGTEL_SERVER**

This parameter stores the URL value my.pingtel.com after the MyPingtel Sign-In xpression application registers a phone for the MyPingtel user por-
Set network management parameters

tal. You can review this parameter in the user-config file. Running the MyPingtel Sign-In xpression sets the value for this parameter.

**PHONESET_MYPINGTEL_USERNAME**

This parameter stores the user name entered during the MyPingtel Sign-In process. You can review this parameter in the user-config file. Running the MyPingtel Sign-In xpression sets the value for this parameter.

**Tip** The PHONESET_HTTP_AUTH_DB parameter also stores the MyPingtel user name along with the encrypted password.

### Enabling voice mail message waiting indication

If your network includes a voice mail server that can send SIP NOTIFY messages, the xpressa phones in your network can receive those messages and automatically alert users when voice mail is received or other status changes take place. There are two options for setting up this process:

- Configure the xpressa phone to send a SUBSCRIBE message to the server each time it starts up. The PHONESET_MSG_WAITING_SUBSCRIBE parameter stores the voice mail server’s location. The server can then send SIP NOTIFY messages to the subscribing IP address. Phones with either dynamic (DHCP) or static IP addresses can use this subscription method.

- Configure the voice mail server to send SIP NOTIFY messages to specified IP addresses when a status change occurs. This method is only feasible for phones with static IP addresses.

After you configure either the phones or the server, the xpressa phone will indicate voice mail status on the home screen by displaying either “No Voice Mail” or “New Voice Mail” with the number of new messages. The xpressa phone’s message light turns on when a new message is received.
Basic configuration

You can also simplify user access to the voice mail server for retrieving messages by configuring the PHONESET_VOICEMAIL_RETRIEVE parameter.

**Tip** To define the voice mail server as the destination for incoming calls, see *Setting up call forwarding* on page 57.

**PHONESET_MSG_WAITING_SUBSCRIBE**

This configuration parameter stores the address for subscribing to message waiting status indication for the xpressa phone user’s voice mail box. For example:

`PHONESET_MSG_WAITING_SUBSCRIBE : sip:sub-user@vm.company.com`

The xpressa phone automatically sends a SUBSCRIBE message to the specified address each time it starts up, and resubscribes before the subscription period expires. The voice mail server subsequently sends the phone a NOTIFY message each time the message waiting status changes.

**PHONESET_VOICEMAIL_RETRIEVE**

If you store the retrieval address for a user’s voice mail messages with this parameter, the user can press a single button to dial the voice mail server for message retrieval.

You use the browser-based interface to specify a complete SIP URL for retrieving messages from the target mailbox. Some examples follow.

`sip:sub-username-retrieve-inpin@sipserver`
Set network management parameters

```
sip:username@vm.pingtel.com;function=retrieve
sip:username@voicemail.pingtel.com;msgId=4
```

To determine the appropriate syntax to use in identifying this SIP URL, refer to the documentation supplied with your voice mail server.

If you set a value for this parameter, the user can press the button to the right of the "No Voice Mail" or "New Voice Mail" indicator on the xpressa home screen at any time to dial the voice mail server and retrieve or administer messages.

**Tip** The “New Voice Mail” indicator will still display in response to a SIP NOTIFY message even if you do not set a value for this parameter. However, the user must explicitly dial the voice mail server to retrieve or administer messages.

### Sending SNMP messages

Each xpressa phone has an SNMP agent and can be used in an SNMP (Simple Network Management Protocol) network management system. The xpressa phone’s SNMP agent supports versions 1 and 2c of the SNMP protocol.

Network management stations manage xpressa phones by directing read and write requests to a phone’s IP address. You do not need to specifically configure the xpressa phones for SNMP; however, for an xpressa phone to send trap messages to a network management station you set the `PHONESET_SNMP_TRAP_DESTS` parameter.

### SNMP read requests

The xpressa phone SNMP agent provides read-only access to the following MIB-II (Internet Management Information Base) manageable object groups:

- system
Basic configuration

- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

To retrieve values from these groups a network management station should use either the “pub” or “public” get community strings.

SNMP write requests

Within the MIB-II system group, the xpressa phone SNMP agent allows write access to these variables:

- sysContact
- sysName
- sysLocation

To set writable values a station should use either the “priv” or “private” set community strings.

Note: SNMP changes do not persist over xpressa phone restarts.

PHONESET_SNMP_TRAPDESTS

For the xpressa phone’s SNMP agent to send unsolicited trap messages to a network management station, you supply the IP address or host name of the station as the value for this parameter.

You can specify up to eight stations by entering each host name or IP address separated by a space. For example:

PHONESET_SNMP_TRAPDESTS : 102.69.145.2 sip.pingtel.com
When you use the browser-based interface, enter the host names and addresses on a single line, separated by spaces:

```
10.1.69.145.2 asy.pingtel.com
```

**Selecting an Ethernet duplex mode**

Duplexing offers performance options for how packets are sent and received over the network. The duplex modes are:

- **Half-duplex**, which uses repeater hubs to perform one send or receive operation at a time.
- **Full-duplex**, which uses switching hubs to send and receive packets at the same time.

The **PHONESET_NETWORK_DUPLEX** parameter provides control over the Ethernet duplex mode used by xpressa phones.

**PHONESET_NETWORK_DUPLEX**

This parameter identifies which Ethernet duplex mode the xpressa phone should use: either HALF or FULL. The default is HALF.

To change the value for this parameter you use the browser-based interface described on page 26. Changes to this parameter should be made only by a system administrator or network engineer who is fully aware of the implications and consequences of such a change. In the browser-based interface, click **Administration: Phone Configuration** then scroll to the Additional Parameters text box at the bottom of this page.

**Note** This parameter does not apply to the instant xpressa softphone.
Basic configuration

Define an image for the home screen

You can present a corporate logo or other graphic image on the home screen of xpressa phones. For example:

![Home screen image](image.png)

To do so, you:

1. Store the image file on a web server in your network.
2. Set the `PHONESET_LOGO_URL` parameter on the xpressa phone(s) to indicate the URL for that file's location.

**PHONESET_LOGO_URL**

This configuration parameter stores the URL of an image file. If defined, the xpressa phone displays the specified image on its home screen. For best results, the image file:

- Must be in .GIF or .JPG format.
- Should be no larger than 24 x 126 pixels.

You use the xpressa phone's browser-based interface to define a value for `PHONESET_LOGO_URL`.

For more information on designing images for display on the xpressa phone, see *The xDK Guidelines for User Interface Design*. 
Setting up Pingtel SIP phone environments

This section provides background information to help you implement Pingtel's SIP phones. Variables and requirements of SIP call type environments are described in two main sections:

- SIP servers: defines the different types of SIP servers and how you set up xpressa phones to use them.
- Call addressing: beginning on page 78, describes how call requests are routed in different SIP environments.

Additional background information on the Session Initiation Protocol (SIP) is provided in an appendix. See page 148.

SIP servers

Servers in a SIP call environment are application programs that accept requests and make responses. In an environment with xpressa phones, you can set up SIP servers in your own IP network, or contract with a SIP telecommunications service provider for access to SIP servers on a hosted basis. The different types of SIP servers are:

- Registry
  A Registry server maintains a database that maps an extension, telephone number, or other user identifier to the IP address that identifies a SIP phone. An xpressa phone can provide its IP address and assigned extension to a Registry server automatically.

- Directory
  A server that provides location services for addressing call requests is a Directory server. Directory servers are also known as Location servers. In a SIP environment that uses xpressa phones, you will usually set up a Directory server. Any Proxy or Redirect server can be a Directory server.
Setting up Pingtel SIP phone environments

- **Proxy**
  A Proxy server is an intermediary program that accepts SIP call requests, optionally performs services, and then passes the request on.

- **Redirect**
  A Redirect server, like a Proxy server, is an intermediary program that intercepts SIP call requests and can optionally perform services for the request. However, a Redirect server then returns the request to the originator of the call.

These servers can be located at the same or different addresses, within or outside of your organization’s network.

**Registry server**

A SIP Registry server provides a database of identifying information for the xpressa phones in an installation. To build and maintain this database automatically, each xpressa phone can periodically register by sending its IP address and assigned extension (in the form of a SIP URL) to the Registry server.

To set up xpressa phones to use a Registry server

Configure each xpressa phone to provide values for these parameters:

- A unique extension. See `PHONESET_EXTENSION` on page 46.
- The address of the Registry server. See `SIP_REGISTRY_SERVERS` on page 86.
- A time limit in seconds within which the xpressa phone must reregister with the Registry server. See `SIP_REGISTER_PERIOD` on page 86.

Registration can take place as frequently or infrequently as you wish. By default, each xpressa phone registers hourly (every 3600 seconds).

Using this information, an xpressa phone periodically registers its SIP URL in the format `sip:<extension>@<registry server>`.
Directory server

Pingtel uses the term Directory server for any Proxy or Redirect server that provides location services to help improve the addressing of call requests in a SIP call type environment. A Directory server may also be called a SIP Location server.

If you configure the xpressa phones in your environment to use a Directory server, phone users can dial a series of digits (that is, a telephone number or extension) instead of always dialing a SIP URL when they wish to make a call. When a Proxy server or Redirect server is designated a Directory server, the service that it provides is to improve call request addressing. For more information on call addressing, see page 78.

**Tip** The Directory server accesses a database of SIP URLs for xpressa phones and the extensions or telephone numbers that correspond to them. When you configure the xpressa phones to register with a Registry server this database is kept up to date automatically.

**To set up xpressa phones to use a Directory server**

The `SIPDIRECTORY_SERVERS` configuration parameter stores the address of the Proxy or Redirect server that acts as the Directory server. When you define this address on an xpressa phone, all call requests made from that phone are routed through the Directory server. For more information see page 85.

Illustrations of different Directory server configurations follow.
Setting up Pingtel SIP phone environments

Proxy server as Directory server

In this SIP environment, a Proxy server acts as the Directory server:

When a SIP call request is routed to the Proxy server (1), the service that the Proxy server provides is a lookup to improve call addressing (2). After the Proxy/Directory server performs this service it automatically sends the call request on to the target address (3).

For more information on Proxy servers see page 77.
Redirect server as Directory server

This SIP environment has a Redirect server acting as the Directory server:

When a SIP call request is routed to a Redirect server for location services (1), the Redirect/Directory server performs the lookup (2) and then returns the call request to the originating phone (3) with the results of the lookup. The call request is then automatically readdressed and sent on to the target address (4).

For more information on Redirect servers see page 77.
Setting up Pingtel SIP phone environments

In this illustration, a Directory server performs both Proxy and Redirect services:

1. Call request (1)
2. Directory lookup (2)
3. Proxied request (3)
4. Busy (4)
5. Redirect (5)
6. Redirected request (6)

When the Directory server receives a call request (1), it performs a lookup to improve call addressing (2) and then acts as a Proxy server and forwards the invitation on to the target (3).

In a case where the target is busy, the Directory server receives the busy response (4) and again attempts to find a more precise address for the call. It then acts as a Redirect server and sends the message back to the originating xpressa phone (5) so that a new call request can be sent (6).
Proxy server

A SIP Proxy server is an intermediary program that makes requests on behalf of clients (xpressa phones). In an xpressa phone environment, SIP Proxy servers can:

- Provide directory services. You use the `SIP_DIRECTORY_SERVERS` configuration parameter to store the address of the SIP Proxy server that provides directory services.
- Route messages through a firewall. You use the `SIP_PROXY_SERVERS` configuration parameter to store the address of the SIP Proxy server that provides firewall routing services.

Most xpressa phone environments include a single SIP Proxy server that provides directory services for xpressa phones. A separate, additional SIP firewall proxy server usually is not defined.

**Tip** Your environment may also include SIP Proxy servers that provide additional network features or capabilities. You do not need to configure xpressa phones with the addresses of such Proxy servers.

**To set up xpressa phones to use a Proxy server**

To configure an xpressa phone to store the address of a SIP firewall proxy server, you use `SIP_PROXY_SERVERS`.

**Note** Provide an address for this parameter only if your environment includes a separate Proxy server that provides a service other than location services. For an illustration of a SIP environment that includes both a Proxy server and a Directory server, see page 83.

Redirect server

A SIP Redirect server is an intermediary program that intercepts SIP call requests, optionally performs services for the request, and then returns the
Setting up Pingtel SIP phone environments

request to the caller regardless of the address in the message’s To field. Redirect servers generally validate the location of a call addressee.

Here’s an illustration of a SIP environment with a Redirect server:

A Redirect server receives a SIP call request (1), performs a service for the request, and then returns the request to the originator of the call (2). The xpressa phone then resends the call request automatically (3).

Call addressing

Whenever you make a telephone call, you provide an address for the call.

- In traditional telephone systems, the address is a series of digits, such as an extension number or telephone number.
- In a SIP call type environment, the address must conform to the SIP standard, which requires call addresses to be SIP URLs such as sip:10.1.1.105 or sip:jwayne@truegrit.com.

For your users to address calls in a SIP environment, you can require them to enter complete alphanumeric SIP URLs each time they dial, or you can
provide a more familiar means of addressing telephone calls by dialing only digits. There are two ways of accomplishing this:

- Each user can set up a local database of speed dial numbers that correspond to SIP URLs.
- You can provide an installation-wide database of numbers that correspond to SIP URLs. This database is managed by the SIP Registry server, and accessed by the SIP Directory server.

**Dialing a SIP URL**

Individual users can enter complete, alphanumeric SIP URLs on the xpressa phone to address call requests. For information on dialing by URL, see Using Pingtel phones.

**Dialing speed dial numbers**

Individual users can set up and maintain independent databases of SIP URLs and corresponding numeric identifiers on each xpressa phone by setting up speed dial numbers.

When a user dials a speed dial number, the list of stored speed dial numbers is checked for that value. If a match is found, the call request is addressed with the previously-defined SIP URL.

**Tip** Users can define speed dial numbers that correspond to telephone numbers. To address calls made using these speed dial numbers, the phone must use the location services of other network servers to translate that number into a SIP URL. See page 80.

For information on setting up and dialing speed dial numbers, see *Using the xpressa phone* in Using Pingtel phones.
Setting up Pingtel SIP phone environments

Message flow: SIP URL or speed dial number

This illustration shows the message flow of a call request that is addressed with a SIP URL or a speed dial number:

![](image)

**Dialing extensions and telephone numbers**

You can also set up an installation-wide database of SIP URLs and numbers on a network SIP server, called a Directory server. After this database is set up, you store the address of the Directory server in the configuration file of each xpressa phone using the `SIP_DIRECTORY_SERVERS` parameter.

When a user dials a series of digits, the xpressa phone actually addresses the call like this: `sip:<digits dialed>@<Directory server address>` to send the message to the Directory server. The Directory server checks its database for a match to the digits dialed. If a match is found, the Directory server addresses the request with it.

**Tip** The above example assumes that the xpressa phone does not have any digit maps that match the dialed digits. If such a digit map exists, it overrides this default procedure for call addressing.

A Directory server can be a Proxy server, a Redirect server, or both. For more information on the different types of SIP servers, see page 71.
Message flow: Proxy server as Directory server

The diagram on page 74 shows the message flow of a call request that uses a Directory server for addressing. In this illustration, a Proxy server is the Directory server. When a user dials a series of digits:

1. The call request is routed automatically to the Directory server.
2. The Directory database is checked for a SIP URL to match the dialed numeric string.
3. The call request is readdressed with the resulting SIP URL and forwarded.

Message flow: Redirect server as Directory server

The diagram on page 75 illustrates the message flow of a call request that uses a Directory server for addressing. In this illustration, a Redirect server is the Directory server. When a user dials a series of digits:

1. The call request is routed automatically to the Directory server.
2. The Directory database is checked for a SIP URL to match the dialed numeric string.
3. The resulting SIP URL address is returned to the xpressa phone that originated the call request.
4. The xpressa phone automatically creates a new call request and sends it to the SIP address.
Setting up Pingtel SIP phone environments

Routing calls through additional servers

Further configuration choices are possible if you define additional servers in your environment.

At your installation, call requests from the xpressa phone may need to traverse one or more Proxy servers to reach the Directory server, other SIP phones, or both. Such additional Proxy servers are analogous to HTTP Proxy servers, and allow SIP messages to be proxied through a firewall.

To route SIP call requests correctly in these environments, you configure each xpressa phone with an address for the Proxy server. Store this address using the `SIP_PROXY_SERVERS` parameter. When set, every SIP request, including those that are addressed with a speed dial ID or a SIP URL, are routed through the defined Proxy server.

If both a Proxy server and a Directory server are defined, when a call request that requires the location services of the Directory server is made it is routed to the Proxy server before it is sent on to the Directory server:
With this server configuration, a SIP call request is sent first to the Proxy server (1), which provides services as defined. The request is then forwarded to the Directory server (2) which provides the lookup service (3). In this illustration, a Proxy server acts as the Directory server, so it sends the call request on to the target address automatically (4).

**Tip** In this environment, you provide different addresses for the `SIP_PROXY_SERVERS` and `SIP_DIRECTORY_SERVERS` on the xpressa phone. In environments that have a single Proxy server to provide location services, you store its address as the `SIP_DIRECTORY_SERVERS` parameter only.

**Proxy, Directory, and Redirect servers defined**

Another configuration that may suit your installation is to establish one or more additional Proxy servers, and make the Directory server a Redirect server.
Setting up Pingtel SIP phone environments

To route SIP call requests correctly, you configure each xpressa phone with an address for the Proxy server and a different address for the Directory server. Use the SIP_PROXY_SERVERS and SIP_DIRECTORY_SERVERS parameters to store these addresses.

\textit{Note:} A Directory Server can proxy messages, redirect messages, or both.

In this environment, SIP call requests are routed first to the Proxy server (1) which provides services as defined. The Proxy server forwards the request to the Directory server (2) which provides the lookup service (3). In this illustration, the Directory server is a Redirect server, so it returns the call request back to the originator by way of the Proxy server (4), (5). The call request is then automatically readdressed and resent to the target address, again by way of the Proxy server (6), (7).
### Configuring phones for SIP environments

This section describes the configuration parameters that you set to:

- Identify SIP servers: see below.
- Complete SIP messaging: see page 87.
- Send authentication data with outgoing calls: see page 89.
- Require authentication for incoming calls: see page 92.

For information on how to change these configuration parameters with the browser-based interface see page 24.

#### Identify SIP servers

These configuration parameters define addresses and other characteristics of the SIP Directory, Registry, and Proxy servers in your SIP environment. Generally, you define the same values for these parameters on all xpressa phones at your installation. To set values for these parameters, use the browser-based interface or edit the `pinger-config` file.

For more information on SIP servers see page 71.

### Defining the SIP Location server

**SIP_DIRECTORY_SERVERS**

This parameter stores the address of the SIP Proxy or Redirect server that provides location services for call requests by converting dialed telephone numbers into SIP addresses. Generally, you enter the value for this parameter in the form of a fully qualified host name, using the format `sip:<host name>`. For example, in the `pinger-config` file you enter:

```
SIP_DIRECTORY_SERVERS : sip:sip.pingtel.com
```

If a Registry server is used, it is often the same as the Directory server. For more information, see page 73.
TipDialed digits are compared to the digit maps configured for an xpressa phone before a call request is sent to the Directory server. If a matching digit map is found, the request uses that address. For information on how to supply different server addresses based on dialed digits, see PHONESET_DIGITMAP on page 48.

Setting up SIP registration

SIP_REGISTRY_SERVERS
This parameter stores the address of the Registry server to which the xpressa phone will send its SIP URL. Normally, you enter this address in the format sip:<domain name>. The phone automatically registers its SIP URL in the format sip:<extension>@<registry server>.

If a Directory server is used, it is often the same as the Registry server. For more information, see page 73.

SIP_REGISTER_PERIOD
This parameter defines the number of seconds until the xpressa phone’s registration with the Registry server expires. The xpressa phone automatically re-registers itself before this time period elapses, or before the Registry server’s period elapses if it is shorter.

The supplied default for this parameter is 3600 (seconds, or one hour).

SIP_ADDRESS
If you do not define a SIP Registry server, the xpressa phone uses the format sip:<extension>@<phone IP address> to include its address as the From URL in all SIP messages. To send a different address as the From URL, such as a fully qualified host name, store that address as the SIP_ADDRESS. The phone will send its address in the format sip:<extension>@<SIP_ADDRESS>.
Defining an additional Proxy server

You can set up a Proxy server that is analogous to an HTTP Proxy server to provide firewall services in your SIP environment. Generally, you set up this type of SIP firewall proxy server in addition to, and not in place of, a Proxy server that provides location services (a Directory server).

If you define both a Directory server (using the `SIP_DIRECTORY_SERVERS` parameter on page 85) and a SIP firewall proxy server (using `SIP_PROXY_SERVERS`), calls go through the SIP firewall proxy server even to get to the Directory server. Typically, you define only a Directory server.

`SIP_PROXY_SERVERS`

If all outbound calls must go through a Proxy server (similar to a firewall), this parameter stores the address of that server. Generally, you enter the address of a SIP firewall proxy server as a fully qualified host name using the format `sip:<host name>`. For example:

```
SIP_PROXY_SERVERS : sip:sip.pingtel.com
```

To route all requests from an xpressa phone through a specific port as well as the Proxy server, enter both the Proxy server’s IP address and its port:

```
SIP_PROXY_SERVERS : sip:171.71.141.7:12345
```

**Note** Do not use this parameter to store the address of a server that provides location services. Use `SIP_DIRECTORY_SERVERS` to store that address.

SIP messaging parameters

The SIP messaging parameters define the TCP and UDP ports on which SIP messages are expected, and enables session reinvite messaging.

To set values for these parameters, use the browser-based interface or edit the `pinger-config` file.
Configuring phones for SIP environments

**Defining ports for SIP messages**

*SIP_TCP_PORT  
SIP_UDP_PORT*

These parameters define the IP ports on which SIP TCP and UDP messages are expected. The supplied default for both parameters is 5060, the well-known port number for SIP messages.

**Tip** Values other than 5060 may be entered. However, setting the TCP and UDP ports to values that are not the same may result in undesirable behavior.

**Enabling session timer**

*SIP_SESSION_REINVITE_TIMER*

This parameter enables sending of session reinvite messages by the xpressa phone during calls. To enable this feature, you define the number of seconds between such messages. Session reinvite messages can help a Proxy server that performs call monitoring services track the duration of ongoing calls.

- All phones participating in a call must support SIP session reinvite for these messages to be sent.
- If the other phone(s) or the Proxy server has different time period settings for the interval between session reinvite messages, the shortest time period is used.

For more information on the SIP session timer extension, see the IETF draft publication “SIP Session Timer.”

**Authentication parameters**

To set values for call authentication, use the browser-based interface or edit the `pinger-config` file.
Setting up authentication for outgoing calls

SIP allows an organization to limit incoming calls to those made by a pre-defined set of authorized users with valid passwords. When a SIP user agent or SIP Proxy server is configured to require authentication, it challenges the xpressa phone that is sending the call request for a user name and password. You can automate the response to such a challenge by storing the user name, password, and destination in two parameters: `SIP_AUTHORIZE_USER` and `SIP_AUTHORIZE_PASSWORD`.

**Note** You must configure both of these parameters.

**SIP_AUTHORIZE_USER**

This parameter stores two values for outgoing calls: the realm identifier or SIP URL of the destination that requires authentication and the assigned, authorized user name for the xpressa phone to supply when calls are made to it. To store both values, you enter the realm identifier or SIP URL, space, colon (:), space, user name.

**Tip** This parameter stores the user name. Use `SIP_AUTHORIZE_PASSWORD` to store the password.

**To enter the destination realm identifier**

For a destination that provides the same authorized user name and password for you to access all of the SIP users within a realm, you set up a single line with just the realm and that authorized user name. To supply a realm identifier, you use the format:

```
SIP_AUTHORIZE_USER.<realm id>
```

If you store a SIP URL for this parameter, it should match the SIP URL in the “To” field of the SIP INVITE message. Use the format:

```
<SIP user id>@<SIP user agent server>
```
Configuring phones for SIP environments

For example, in the `pinger-config` file enter:

SIP_AUTHORIZE_USER.lucille@10.1.1.58

**To enter the user name**

After the realm identifier or SIP URL, enter the authorized user name; that is, the ID you have been given to access the destination. The two values should be separated by a space, a colon (:), and another space. For example, use the browser-based interface to enter:

When you use the browser-based interface, you supply only the realm identifier, without the parameter name. For example, to set up the user name for all SIP user agents within the realm “acme”, enter:

`acme : generalUser1d`

Use an individual line for each realm : user name pair.

**When the destination requires individual user names**

For a destination that requires a different authorized user name and password for each of its SIP user agents, you set up an individual line for each SIP URL at that address along with the assigned user name. For example, a `pinger-config` file might contain three different SIP addresses at the same domain, with three different user names:

SIP_AUTHORIZE_USER.wecoyote@looneytunes.com : Wile_E
SIP_AUTHORIZE_USER.roadrunner@looneytunes.com : ACME
SIP_AUTHORIZE_USER.bugs@looneytunes.com : wabbit

**When the destination accepts a general user name**

For a destination that provides the same authorized user name and password for you to access all of its SIP users, you can set up a single line with just the general SIP user agent server portion of the destination SIP URL and that authorized user name. For example, to set up the user name for
all SIP user agents at the destination sip.acme.com, use the browser-based interface to enter:

```
sip.acme.com : generalUserId
```

You must also define the password for a SIP URL that requires authentication. Use the `SIP_AUTHORIZE_PASSWORD` parameter to store the URL and that password.

**SIP_AUTHORIZE_PASSWORD**

For outgoing calls, stores two values: the realm identifier or SIP URL of the destination that requires authentication and the password for the xpressa phone to supply when calls are made to it. If you supply the realm identifier with the user name using `SIP_AUTHORIZE_USER`, you also supply it with the password:

```
SIP_AUTHORIZE_PASSWORD.<realm id> : <password>
```

To enter these values, you enter the realm identifier or SIP URL, space, colon (:), space, password. Use an individual line for each realm : password pair.

**Note** This parameter stores the password. Use the `SIP_AUTHORIZE_USER` parameter to store the user name.

**When the destination requires individual passwords**

For a destination that provides a different authorized password for each of its SIP user agents, you set up an individual line for each SIP URL at that address along with the assigned password.

For example, a `pinger-config` file might contain three different SIP addresses at the same domain, with three different passwords:

```
SIP_AUTHORIZE_PASSWORD.wecoyote@looneytunes.com : opensesame
SIP_AUTHORIZE_PASSWORD.roadrunner@looneytunes.com : beepbeep
SIP_AUTHORIZE_PASSWORD.bugs@looneytunes.com : carrots
```
Configuring phones for SIP environments

When the destination accepts a general password

For a destination that provides the same authorized password for you to access all of its SIP users, you can set up a single line with just the general SIP user agent server portion of the destination SIP URL and its password. For example, using the browser-based interface you might enter:

```
10.1.1.103 : password
sip.acme.com : generalpassword
```

You must also identify the authorized user name for a SIP URL that requires authentication. Use the `SIP_AUTHORIZE_USER` parameter to store the URL and that user name.

Authenticating incoming calls

SIP allows a user agent (that is, a phone) to limit incoming calls to those made by a predefined set of authorized users with valid passwords. To set up these limits for an xpressa phone, you provide values for three parameters: `SIP_AUTHENTICATE_SCHEME`, `SIP_AUTHENTICATE_REALM`, and `SIP_AUTHENTICATE_DB`.

Tip HTTP authentication is the model for SIP authentication.

**SIP_AUTHENTICATE_SCHEME**

Defining a value for this parameter enables authentication for incoming calls. For incoming calls, defines the encoding used for the password. Options are BASIC and DIGEST, which correspond to the standard HTTP schemes.

**SIP_AUTHENTICATE_REALM**

For incoming calls, stores a text string to define the name of the realm to which authentication applies. For example:

```
SIP_AUTHENTICATE_REALM : ENTERPRISE
```

A value is required if `SIP_AUTHENTICATE_SCHEME` is set.
**SIP_AUTHENTICATE_DB**

For incoming calls, stores an authorized caller name and passwords. Enter the user ID, space, colon (:), space, password:

```
SIP_AUTHENTICATE_DB.(user id) : (password)
```

For example:

```
SIP_AUTHENTICATE_DB.pingtel : topsecret
```

**Tip** The user IDs must not themselves contain spaces, tabs, or colons.

You can set up more than one user ID and password by setting up an individual line for each user ID-password pair.
Working with firewalls and NAT

For an xpressa phone to make calls to parties on the other side of a firewall, you configure both the firewall and the xpressa phone.

- If your firewall is packet-based, you configure both the firewall and the xpressa phones to identify the ports that allow incoming VoIP traffic (SIP, RTP, and RTCP packets) to pass through it.
- If your firewall uses NAT (Network Address Translation) and is packet-based, you configure both the firewall and the xpressa phones to identify the firewall's external or Internet IP address in addition to identifying the ports for incoming VoIP traffic. See page 97.
- A proxy-based firewall must use a SIP-specific proxy. See page 99 for tips to help you set up xpressa phones in your installation.

Configure the firewall

This section provides an overview of the tasks that you will complete for your packet-based firewall when you prepare to use xpressa phones. Refer to the documentation provided with your firewall software for instructions.

Recording the external IP address

While you are working with the server or router that provides your firewall services, determine and record its external or Internet IP address. This address may be identified as the WAN IP address, or with another label.

There is no need to change this value for the firewall; however, you do need to configure the xpressa phone to use this IP address as the value for its PHONESET_EXTERNAL_IP_ADDRESS parameter.

Opening VoIP ports

On your firewall, you define the ports to open for incoming SIP, RTP, and RTCP traffic.
Configure the xpressa phone

- The SIP (Session Initiation Protocol) port is used for call control: setting up and tearing down calls. For SIP packets you define a single port. The well known port number for SIP is 5060.
- The RTP (Real-time Transport Protocol) port receives the audio for a call, and the RTCP (Real-time Control Protocol) port receives the control and media statistics stream. Two consecutively numbered ports are required per call to receive these packet streams. The default value for the first port is 8766.
  To allow the xpressa phone user to place calls on hold or make conference calls, four pairs (eight ports) are recommended; at a minimum, two ports are needed to support a single connection.

When you set up these ports for your firewall it may look like this:

<table>
<thead>
<tr>
<th>Port #</th>
<th>Port #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5060</td>
</tr>
<tr>
<td>2</td>
<td>8766</td>
</tr>
<tr>
<td>3</td>
<td>8767</td>
</tr>
<tr>
<td>4</td>
<td>8768</td>
</tr>
<tr>
<td>5</td>
<td>8769</td>
</tr>
<tr>
<td>6</td>
<td>8770</td>
</tr>
<tr>
<td>7</td>
<td>8771</td>
</tr>
<tr>
<td>8</td>
<td>8772</td>
</tr>
<tr>
<td>9</td>
<td>8773</td>
</tr>
</tbody>
</table>

Note The RTP ports that you specify for use by an xpressa phone must be consecutive.

If your firewall has NAT, see page 97 for additional information.

Configure the xpressa phone

Once you have identified the external IP address and opened ports for the incoming VoIP traffic on your packet-based firewall, you configure the xpressa phone to use those same values. Use the phone's browser-based interface to:
Working with firewalls and NAT

- Identify the external IP address.
- Set the SIP port.
- Set the RTP/RTCP ports.

**Identifying the external IP address**

**PHONESET_EXTERNAL_IP_ADDRESS**

This parameter applies to all xpressa phones that make calls through a firewall. You supply an IP address that is outside of the firewall as the value for this parameter. For example:

209.251.66.16

In a configuration file, this address appears as follows:

**PHONESET_EXTERNAL_IP_ADDRESS** : 209.251.66.16

Your xpressa phone includes this IP address in the SIP messages it sends to other SIP user agents to indicate that this is the address to which SIP, RTP, and RTCP packets should be sent.

**Setting the SIP port**

To define the SIP port you set two different parameters to the same value. Both **SIP_TCP_PORT** and **SIP_UDP_PORT** must be set to the phone’s assigned SIP port number. See page 88 for more information on these parameters.

**Setting the RTP/RTCP ports**

The **PHONESET_RTP_PORT_START** parameter identifies the first in a pair of consecutively numbered ports. RTP and RTCP use these ports to receive audio media and control information for each concurrent connection. The starting port defaults to 8766. You do not need to explicitly set the next port. See page 103 for more information on this parameter.

**Tip** You can open several pairs of consecutively numbered ports on your
firewall to support more than one concurrent call. If so, you still define only the starting RTP/RTCP port on the xpressa phone with this parameter.

**Work with a firewall with NAT**

If you are using multiple xpressa phones behind a firewall with NAT, and if that firewall has only a single external IP address, you must open a unique set of external SIP and RTP/RTCP port/address pairs for each phone that makes calls through the firewall.

When you set up these ports for your firewall, you associate the xpressa phone’s IP address with each one. This process is sometimes called port mapping; that is, mapping a port on the external or public side of the firewall to a specific port and device IP address inside the firewall.

If you set up your firewall to allow an xpressa phone with an IP address of 192.168.0.3 to make and receive calls, it may look like this:

<table>
<thead>
<tr>
<th>Port #</th>
<th>Server IP Address</th>
<th>Port #</th>
<th>Server IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5060</td>
<td>6</td>
<td>8770</td>
</tr>
<tr>
<td>2</td>
<td>8766</td>
<td>7</td>
<td>8771</td>
</tr>
<tr>
<td>3</td>
<td>8767</td>
<td>8</td>
<td>8772</td>
</tr>
<tr>
<td>4</td>
<td>8768</td>
<td>9</td>
<td>8773</td>
</tr>
<tr>
<td>5</td>
<td>8769</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note** The RTP ports specified for an xpressa phone must be consecutive.

However, when you have multiple xpressa phones behind the firewall, you use different ports for each one. For example, open unique SIP port 5060 for phone A, port 5061 for phone B, and 5062 for phone C. Then open a range of eight unique, consecutive RTP/RTCP ports for each phone: 8000 to 8007 for phone A, 8008 to 8015 for phone B, 8016 to 8023 for phone C.
Working with firewalls and NAT

The configuration for your firewall may look something like this:

IP address for  
phone A: 192.168.0.3  
phone B: 192.168.0.4  
phone C: 192.168.0.5

<table>
<thead>
<tr>
<th>Port #</th>
<th>Server IP Addr</th>
<th>Port #</th>
<th>Server IP Addr</th>
<th>Port #</th>
<th>Server IP Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5060 192.168.0.3</td>
<td>10</td>
<td>5061 192.168.0.4</td>
<td>19</td>
<td>5062 192.168.0.5</td>
</tr>
<tr>
<td>2</td>
<td>8000 192.168.0.3</td>
<td>11</td>
<td>8008 192.168.0.4</td>
<td>20</td>
<td>8016 192.168.0.5</td>
</tr>
<tr>
<td>3</td>
<td>8001 192.168.0.3</td>
<td>12</td>
<td>8009 192.168.0.4</td>
<td>21</td>
<td>8017 192.168.0.5</td>
</tr>
<tr>
<td>4</td>
<td>8002 192.168.0.3</td>
<td>13</td>
<td>8010 192.168.0.4</td>
<td>22</td>
<td>8018 192.168.0.5</td>
</tr>
<tr>
<td>5</td>
<td>8003 192.168.0.3</td>
<td>14</td>
<td>8011 192.168.0.4</td>
<td>23</td>
<td>8019 192.168.0.5</td>
</tr>
<tr>
<td>6</td>
<td>8004 192.168.0.3</td>
<td>15</td>
<td>8012 192.168.0.4</td>
<td>24</td>
<td>8020 192.168.0.5</td>
</tr>
<tr>
<td>7</td>
<td>8005 192.168.0.3</td>
<td>16</td>
<td>8013 192.168.0.4</td>
<td>25</td>
<td>8021 192.168.0.5</td>
</tr>
<tr>
<td>8</td>
<td>8006 192.168.0.3</td>
<td>17</td>
<td>8014 192.168.0.4</td>
<td>26</td>
<td>8022 192.168.0.5</td>
</tr>
<tr>
<td>9</td>
<td>8007 192.168.0.3</td>
<td>18</td>
<td>8015 192.168.0.4</td>
<td>27</td>
<td>8023 192.168.0.5</td>
</tr>
</tbody>
</table>

You must also make sure that each phone’s SIP_TCP_PORT, SIP_UDP_PORT, and PHONESET_RTP_PORT_START parameters reflect these values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Phone A 192.168.0.3</th>
<th>Phone B 192.168.0.4</th>
<th>Phone C 192.168.0.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_TCP_PORT</td>
<td>5060</td>
<td>5061</td>
<td>5062</td>
</tr>
<tr>
<td>SIP_UDP_PORT</td>
<td>5060</td>
<td>5061</td>
<td>5062</td>
</tr>
<tr>
<td>PHONESET_RTP_PORT_START</td>
<td>8000</td>
<td>8008</td>
<td>8016</td>
</tr>
</tbody>
</table>
Work with a proxied firewall

For xpressa phones to work in an environment with a proxy-based firewall, the firewall must have a SIP-specific proxy implemented. Refer to the documentation provided by your firewall vendor for instructions on how to configure its SIP features.

Configuring phones for a SIP firewall proxy

For xpressa phones to work with a SIP firewall proxy, you are likely to need to set the `SIP_PROXY_SERVERS` parameter to the internal IP address of your SIP firewall proxy.

Depending on the requirements of the SIP firewall proxy that you use, you may also need to configure the xpressa phones by setting one or more of the following parameters:

- `PHONESET_HTTP_PROXY_HOST` and `PHONESET_HTTP_PROXY_PORT`: see below.
- `PHONESET_EXTERNAL_IP_ADDRESS`: see page 96.
- `SIP_TCP_PORT` and `SIP_UDP_PORT`: see page 88.
- `PHONESET_RTP_PORT_START`: see page 103.

Using HTTP proxy settings

`PHONESET_HTTP_PROXY_HOST`  
`PHONESET_HTTP_PROXY_PORT`

An xpressa phone uses HTTP to download software upgrades and xpression application .JAR files. If these HTTP transactions have destinations on a remote server and must go through a proxied firewall, you may need to set values for the `PHONESET_HTTP_PROXY_HOST` and `PHONESET_HTTP_PROXY_PORT` parameters to allow those xpressa phones to originate the HTTP transactions. Examples for these parameters follow.
Working with firewalls and NAT

PHONESET_HTTP_PROXY_HOST : httpproxy.pingtel.com
PHONESET_HTTP_PROXY_PORT : 8080

You set these values with the browser-based interface described on page 26 or by editing the user-config file. If you do not provide values for these parameters, the xpressa phone does not use a proxy.

For information on downloading xpression JAR files, see Working with xpression applications in Using Pingtel phones.
Supporting QoS techniques

This section describes the QoS features of xpressa phones. You can use these features if your network includes an intelligent IP router or Ethernet switch that supports Quality of Service (QoS) techniques.

The QoS techniques supported by xpressa phones are:

- Type of service (TOS) bit marking for IP packets.
- VLAN 802.1p tagging for frame prioritization on Ethernet networks.
- Configuration parameters identifying RTP/RTCP ports for packet prioritization.

TOS bit markings

In order to differentiate classes of service for Internet traffic, each IP packet can include a type of service (TOS) indication to designate the forwarding treatment that it should receive.

- No configuration is needed on the xpressa phones to enable this feature. xpressa phones automatically send the TOS indication for reduced latency (delay) with all RTP and RTCP packets.
- Smart Ethernet switches or routers must be configured to observe these indications and give them preference. Refer to the documentation supplied with your network equipment to take advantage of this feature.

Tip xpressa phones do not support the TOS indication for reliability, as it is of limited usefulness for audio packets.
Supporting QoS techniques

**VLAN 802.1p prioritization**

The 802.1p signaling method sets a prioritization level in the VLAN (Virtual LAN) tag of RTP and RTCP packets, enabling smart switches to give priority to appropriately tagged Ethernet frames.

- Smart Ethernet switches must be configured to support the use of VLAN QoS headers. Refer to the documentation supplied with your equipment to take advantage of this feature.
- By default, the xpressa phone does not send an 802.1p value with the VLAN tags. You use the phonetop interface to set up this QoS feature. Instructions follow.

**Note** Before you implement this feature you should verify that the default gateway and switches in your LAN are configured to support VLAN. If they do not, an xpressa phone that is set to send 802.1p tags will not be able to communicate with any other network device.

To set up 802.1p tagging:

1. Start the Preferences xpression: from the xpressa phone’s home screen, press MORE, then on the Apps tab choose Prefs. You may need to scroll down to find Prefs on this tab.
2. Select the Network Settings category and press Adjust. This task requires the admin password. See page 38.
3. Press to check or clear the Use VLAN QoS check box.
4. Press OK, then restart the xpressa phone. The setting does not take effect until you restart the phone.

**Tip** This network setting is saved on the xpressa phone with other network settings. It is not saved as a configuration parameter.
RTP/RTCP ports

If you set QoS prioritization on your switches and other network devices for specified ports, you can identify the same ports on xpressa phones to prioritize the RTP/RTCP packets that carry audio data.

**PHONESET_RTP_PORT_START**

xpressa phones use a consecutively numbered pair of ports to receive audio media and control information for each concurrent connection. RTP (Real-time Transport Protocol) packets carry audio media, while RTCP (Real-time Control Protocol) packets carry control information. The **PHONESET_RTP_PORT_START** parameter defines the starting port in the RTP/RTCP pair of ports. The default value for this parameter is 8766.

Because an xpressa phone can maintain up to five concurrent connections, a maximum of ten consecutively numbered ports will be identified when you set this parameter:

(1 RTP port + 1 RTCP port) x five connections = 10 ports

This parameter also applies to xpressa phones that make calls through a packet-based firewall. For information on working with firewalls see page 94.

To define port numbers for RTP/RTCP traffic on an xpressa phone you use the browser-based interface described on page 26.
Configuring phones for pingtel.net calling

pingtel.net™ is an Internet-based VoIP calling service that allows xpressa phone users to call PSTN phones and SIP phones that are located outside the xpressa phone user’s local area network. To sign up for this service visit Pingtel’s AppDev Zone at http://appdev.pingtel.com.

When you sign up, you register a specific xpressa phone for the service and provide detailed information about your network and SIP environment.

To begin using the service, you sign in on the xpressa phone. The service then supplies a pinger-config file to the phone. This file contains configuration values that are based on the information supplied during user sign up, including values for firewall and SIP server parameters. As a result, using the pingtel.net service minimizes manual configuration for a registered xpressa phone.

**Note** The pingtel.net calling service is a test network that is intended to promote the use and adoption of SIP products and standards. Pingtel does not plan to offer access to this network to the public at large, and may discontinue the service at any time without notice.

**xpressa phone sign in**

After you register for Pingtel’s AppDev Zone and sign up for the pingtel.net service, you sign in on the xpressa phone. When you sign in you supply:

- The user name you chose for the AppDev Zone.
- Your assigned password. You receive this password via e-mail.

You use the phone’s dial pad to enter the letters in your user name. For information on entering data, see *User interface fundamentals* in Using Pingtel phones.

You can also sign out to stop using the pingtel.net service.
Signing in to pingtel.net

To sign in and start using the pingtel.net calling service, you use the pingtel.net service xpression.

1. From the xpressa phone’s home screen, press MORE, then on the Apps tab choose pingtel.net service.
   You may need to scroll down to find the pingtel.net xpression.

2. Press Next.

3. Use the dial pad to enter your alphanumeric user name.
   Press each button once or more to supply a letter or the number assigned to it. For more information on entering characters on an xpressa phone see User interface fundamentals in Using Pingtel phones.

4. Press Next.

5. Use the dial pad to enter your password.
   Passwords for the AppDev Zone consist of numbers and # or * only.
   Press each button once to supply your password.

6. Press Next.

7. Press Next to accept the supplied pds.pingtel.net/deployment server.
   Currently, only the supplied server name is valid.

8. Restart the xpressa phone.
   The service does not take effect until you restart the phone.

Signing out of pingtel.net

To stop using the pingtel.net calling service:

1. From the xpressa phone’s home screen, press MORE, then on the Apps tab choose pingtel.net service.
Configuring phones for pingtel.net calling

2 Press Sign Out.
   A warning message displays.
3 Press OK.
4 Restart the xpressa phone.

pingtel.net service parameters

This section describes the configuration parameters that relate to the pingtel.net calling service. After sign in, the service supplies values for these parameters automatically each time the xpressa phone restarts.

While you can review these parameters using the browser-based interface, you cannot enable or disable the calling service by changing the values of the parameters described here. To start or stop using the pingtel.net service on an xpressa phone use the phonetop procedures described on page 105.

PHONESET_DEPLOYMENT_SERVER

For an xpressa phone that uses the pingtel.net service, this parameter stores the URL `pds.pingtel.net/deployment`. You supply the value for this configuration parameter when you sign in, as described on page 105.

PHONESET_ADMIN_DOMAIN

Applies only to xpressa phones that use the pingtel.net calling service. Supplied to the phone by the pingtel.net service to identify the administrative domain to which the phone belongs.

PHONESET_LOGICAL_ID

Applies only to xpressa phones that use the pingtel.net calling service. Supplied by the pingtel.net service to identify a key for your xpressa phone. This key is used by the pingtel.net service to determine configuration settings for your device.
Managing xpressa phones

Periodically, you may need to perform maintenance on an xpressa phone such as:

- Installing a software upgrade: see below.
- Managing xpression applications: see page 111.
- Restarting an xpressa phone: see page 113.
- Reverting to the factory default settings: see page 115.
- Installing replacement audio files: see page 117.

This section describes these tasks.

Install software upgrades

Each xpressa phone stores:

- A core software file that contains operating system and application program files.
- Several .JAR files that contain application and required Java files.

When Pingtel releases new software for the xpressa phone, both the core software file and a core application .JAR file must be replaced. One or more additional .JAR files may also be distributed to complete the installation of a new release.

At your installation, you can install new software versions on xpressa phones:

- Automatically, using Pingtel’s VersionCheck xpression application.
- Manually, by installing software distribution files individually.
Managing xpressa phones

**Installing upgrades automatically with VersionCheck**

To automate software upgrades, all xpressa phones are delivered with Pingtel's VersionCheck xpression application pre-installed. Each time an xpressa phone is restarted, VersionCheck verifies that it has the latest operating system and application files available.

When Pingtel releases a new version, VersionCheck presents a prompt that allows any user to upgrade to the new version automatically.

![VersionCheck prompt](Image)

**Note** Do not interrupt the xpressa phone’s connections to power or the network during the upgrade process.

Pingtel's VersionCheck application can only run when a phone has Internet connectivity to Pingtel's application server. If the xpressa phone is behind a firewall that does not allow HTTP access to Pingtel's server, or if VersionCheck is uninstalled or otherwise nonfunctional, it does not run.

**Tip** If your installation uses a proxy-based firewall, set the parameters described on page 99 to use this feature.

**Installing upgrades manually**

If VersionCheck is not available, you can update the operating system and Java files of each xpressa phone manually. When new software is released, Pingtel updates the Support area of the www.pingtel.com web site so that you can download all required files.
Install software upgrades

Note  The xpressa phone does not validate manually loaded files before using them. If you load an invalid file, your phone may become unusable and require repair or replacement by Pingtel.

Determining the current version
To find an xpressa phone’s current software and operating system version numbers:
1  From the xpressa phone’s home screen, press MORE.
2  Select the Menu tab.
3  Select About.
   The software version number displays.
4  Press OK.

Updating software distribution files
To prevent errors, complete all of these steps before you perform other tasks on the xpressa phone. Do not unplug the xpressa phone’s power or network connections during the upgrade process.
1  On the myxpressa home page, click Administration: File Uploads.
   For information on how to access a phone’s myxpressa home page, see page 26.
   A web page for installing and reviewing software files opens.
2  Scroll down to the Software section of this page, then browse for and enter the path and name of the new xpressa operating system (.xos) file that you downloaded.
Managing xpressa phones

3 Click **Upload xpressa core software**.
   An “Upload Successful” message displays in your browser.

4 Click your browser’s Back button, then browse for and enter the path and name of the core Java applications file that you downloaded.

5 Click **Upload xpressa Java software**.
   An “Upload Successful” message displays and the xpressa phone restarts automatically.

6 If required by the software distribution, upload additional Java files.
Repeat step 4 and step 5 using the appropriate text entry box.

7 After installing additional Java files, restart the xpressa phone. See page 113 for instructions.

**Note** Be sure to upload the operating system file first, then the Java file. Otherwise, release installation is not complete and the xpressa phone is not ready for use.

**Manage xpression applications**

Any xpressa phone user can install and remove xpression applications one at a time with the browser-based interface. System administrators can also use this method to manage the xpression applications on individual phones. This process is described in the *Working with xpression applications* section of *Using Pingtel phones*.

To manage xpression applications for more than one phone, or to add or remove more than one xpression application at a time, you may prefer to edit the **app-config** file that stores application location data as needed, then upload it to one or more phones. This process is similar to the way you can work directly with configuration files, as described on page 28.

The **app-config** file is an editable ASCII text file. This file stores the URL locations of the xpression applications you want to run on a given xpressa phone. Each URL goes on an individual line in the format:

```
USER, <URL>
```

An example showing the standard applications supplied with an xpressa phone follows.

```
# Standard Applications
USER, http://appsrv.pingtel.com/pingtelapps/1.2.0/PingtelNet.jar
USER, http://appsrv.pingtel.com/pingtelapps/1.2.0/VersionCheck.jar
USER, http://appsrv.pingtel.com/pingtelapps/1.2.0/PingtelNews.jar
```
Managing xpressa phones

To include comments in the **app-config** file, place the text on a new line that starts with `#`, as shown in the example above.

You use the browser-based interface to review the contents of an xpressa phone’s **app-config** file and to upload edited files.

**Reviewing an app-config file**

1. On the myxpressa home page, click **Administration: File Listing**. For information on how to access this home page see page 26. A list of files stored on the xpressa phone opens.
2. Click **app-config**. The contents of this file display in your browser.

**Editing an app-config file**

1. From the browser’s File menu, select Save As and save the **app-config** data in a plain text (.txt) file on your local PC.
2. Open the saved app-config.txt file in an editor such as Notepad.
3. Edit the file contents to add, delete, or change the location information of the application .JAR files.
   - Use a new line for each application URL.
   - For applications, begin each line USER,
   - For comments, begin each line with `#`.
4. Save your changes.

After you download and edit the **app-config** file for one xpressa phone, you can upload the same file to all phones that need to have the same set of applications installed.

**Tip** You can load a maximum of five xpression applications on an instant xpressa softphone. There is no limit for an xpressa phone.
**Restart an xpressa phone**

**Uploading an edited app-config file**

1. In your browser, click **Administration: File Uploads**.
2. In the Phone configuration section, browse for and enter the name of the edited app-config.txt file.
3. Click **Upload app-config**.
4. Click **Restart** to restart the xpressa phone.

Edit the IP address in your browser's Address or Location field to access a different phone's file upload page, and repeat the process as needed.

**Restart an xpressa phone**

Before an xpressa phone will use a new or changed software or configuration file, it must be restarted. You can restart an xpressa phone:

- From the phonetop user interface.
- By pressing a manual reset switch.
- From the browser-based interface.

The startup process can take up to two minutes to complete. During this time, phone calls cannot be made or received by the xpressa phone.

**Restarting from the phonetop**

1. From the xpressa home screen, press MORE.
   - The start up audio file plays and the xpressa phone splash screen displays.
Managing xpressa phones

When the xpressa home screen displays, the xpressa phone is once again ready for use.

**Restarting manually**

The xpressa phone also offers a manual reset switch that restarts the phone. This switch is located on the bottom of the phone.

A toothpick or other nonconducting tool may be needed to press this switch.

For certain electrostatic discharge (ESD) events, you may need to restart the xpressa phone manually using this switch.
### Revert to factory defaults

**Restarting from a browser**

You’ll find a Restart button on the following myxpressa web pages:

- Preferences: Preferences
- Administration: Phone Configuration
- Administration: File Uploads

To restart an xpressa phone from one of these pages, click to save your changes or perform the upload and then click **Restart**.

**Note** Restarting an xpressa phone interrupts ongoing calls, as well as the phone’s ability to receive and place calls. If you plan to restart an xpressa phone from a remote PC, be sure to warn the phone’s user.

### Revert to factory defaults

You can set an xpressa phone back to its original, default settings. This procedure replaces your customizations to network settings and configuration parameters with default values, and removes all installed xpression applications.

<table>
<thead>
<tr>
<th>Customization type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>network settings</td>
<td>Restored to DHCP. For information on network settings see page 18. Also removes time server and QoS customizations.</td>
</tr>
<tr>
<td>administrative password</td>
<td>Set to null. For information on administrative security see page 38. Also deletes all users set up to use the phone’s browser-based interface.</td>
</tr>
<tr>
<td>configuration parameters and preferences</td>
<td>Restores all configuration parameter values to their supplied defaults. See page 35 for a list of defaults.</td>
</tr>
</tbody>
</table>
Managing xpressa phones

<table>
<thead>
<tr>
<th>Customization type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>pingeitl.net calling service</td>
<td>Sets the pingeitl.net user name and password to null. Sign in with the pingeitl.net service application to supply the correct values after restarting the phone. The pingeitl.net calling service supplies all configuration parameter values each time you restart; if you use this service be sure to restart the phone after you revert to factory defaults.</td>
</tr>
<tr>
<td>xpression applications</td>
<td>Restores the app-config file to the set of default standard applications. For information on installing xpression applications, see page 111 or Working with xpression applications in Using Pingtel phones.</td>
</tr>
<tr>
<td>speed dial numbers</td>
<td>Removed. For information on using the browser-based interface or the phone to set up speed dial numbers, see Using the xpressa phone in Using Pingtel phones.</td>
</tr>
</tbody>
</table>

**Tip** This procedure does not affect the software version used by the phone.

To set a phone back to its original, factory default settings:

1. Optionally, save a copy of the xpressa phone’s pinger-config, user-config, and app-config files.
   
   This preliminary step can help you reconfigure the phone quickly after you revert to factory defaults. For more information see page 29.

2. From the xpressa home screen, press MORE.
   
   A warning message displays.

4. Press OK.
   
   To return to the home screen without making any changes press Cancel.

5. Restart the xpressa phone.
6 Optionally, follow step 7 through step 10 on page 33 to upload the copies you made of `pinger-config`, `user-config`, and `app-config`.

**Install audio files**

Every xpressa phone comes with two audio files that play as the ring tone and at startup. You can replace these files with any other audio file that conforms to these characteristics:

- The file format can be `.WAV`, Sun `.AU`, or `.RAW` audio.
- All formats must be 16 bit signed PCM.
- All formats must use a sampling rate of 8000 samples/second.
- The maximum file size is 500KB.
- `.WAV` files must be mono.
- `.RAW` files must be in little-endian byte order.

In addition, audio files that are used as ring tones should be six seconds in length to match the standard ring length.

**Note** The `.RAW` extension denotes audio files that contain raw PCM audio data with no header information.

You use the browser-based interface to upload an appropriate new audio file to an xpressa phone. To replace an audio file:

1. On the myxpressa home page, click **Administration: File Uploads**. For information on how to access this home page see page 26. A web page for installing and reviewing software files opens.
2. In the Audio section of this page, work with either the ring tone or the startup audio file.
3. Browse for and enter the path and name of the audio file.
Managing xpressa phones

4 Click **Upload**.
   An “Upload Successful” message displays.

5 Repeat step 2 through step 4 for the other audio file if desired.

**Tip** All users can upload a new ring tone file to an xpressa phone from the myxpressa home page. The *admin* log on is not required.
Troubleshooting

This section provides information to help you solve problems with an xpressa phone and work with Pingtel's Technical Assistance Center (TAC) to resolve questions. It also describes tools that may help you learn more about an xpressa phone: see page 128.

Support checklists

Before you contact Pingtel's TAC with a question, perform a preliminary investigation by following one or more of these procedures:

- No dial tone: see page 119.
- LCD display screen is blank: see page 120.
- Buttons do not light or work: see page 120.
- Problems with incoming calls: see page 121.
- Problems with outgoing calls: see page 123.
- One-way conversation: see page 124.
- No access to browser-based interface: see page 125.
- Connection is noisy: see page 126.
- xpression applications don't load or run: see page 126.
- Physical defects: see page 127.

No dial tone

Check the power

Make sure that the xpressa phone is receiving power by checking all of its connections. Verify that the phone is installed appropriately for the available power source (from a power transformer and PIM, or Cisco Inline Power patch panel or switch). Installation is described on page 12.
Troubleshooting

Check the cable
Verify that the Cat 5 cable supplied with the xpressa phone, or another Cat 5 cable with four pairs of wires, is connected to the phone. If a cable with only two pairs of wires is used, replace it with a Cat 5 that has all four pairs.

Compare handset and speakerphone
Try taking the phone off hook with the handset, then compare the result when you use the speakerphone.

Check the handset
xpressa phones ship with a separate, unconnected handset and cord. Make sure the handset is connected to the phone. You can also connect the handset from another xpressa phone to your phone to determine if your handset is defective.

LCD display screen is blank
Check for power and check the cable connected to the phone as described on page 119. An additional procedure follows.

Adjust the contrast
Press the ▼ fixed function button to decrease the contrast level used by the LCD display.

Buttons do not light or work
Check for power as described on page 119. Additional procedures follow.

Verify functionality
The following fixed function buttons should light when in use:
• HEADSET
• MUTE
Support checklists

- **HOLD**
- **SPEAKER**

Other fixed function buttons do not light. Check the functionality of each listed button to determine if the problem is with the LED only.

**Check all buttons**

If one or more of the fixed function buttons listed above does not work as expected, the problem may be due to a mechanical failure. Check the functionality of all buttons, including dial pad buttons, MORE, TRANSFER, and CONF to determine the extent of the problem.

**Problems with incoming calls**

**Adjust the volume**

If an xpressa phone does not ring for incoming calls, make sure that the ringer volume is set to an audible level. On the phonetop, use the Prefs application’s Volume & Contrast category to adjust Ringer Volume.

**Check the call indication method**

Users can turn the ring tone off. If an xpressa phone does not ring for incoming calls, use Preferences in the browser-based interface or the Prefs application to go to the Call Handling category and check the selected call indication method.

**Validate the ring tone file**

If the ring tone file has been replaced by another file, make sure that the new file meets the specifications listed on page 117. If necessary, replace the audio file with another file that meets these standards.
Troubleshooting

Check call handling preferences
Verify that the phone is not set to:
- Forward all calls
- Do Not Disturb mode
See page 55 for information on these call handling parameters.

Restart the phone
Follow the procedures to Restart an xpressa phone on page 113. Restarting may cause configuration changes or new preference settings to take effect.

Check network connection
Ping the phone's IP address or check its TO HUB lights (on the bottom of the phone) to verify the phone's network connection. If there is no connection:
- Check the Cat 5 cable that is connected to the phone as described on page 120.
- If you use the PIM to supply power to the phone, make sure that a Cat 5 also connects the PIM to a 10 Base-T or 10/100 Ethernet/LAN port.

Validate the phone's address
Check the phone's IP address then determine if the phone can receive an incoming call when dialed by URL. Compare the result to incoming calls addressed with an extension or telephone number: if these incoming calls are not received, validate the address mapping performed by a Directory server or digit map to link the phone's extension or telephone number to its IP address.
Verify call authentication settings

Incoming calls for this xpressa phone may be restricted to those made by a predefined set of users with valid passwords. See Authenticating incoming calls on page 92 for information on authorizing callers.

Check firewall configuration

If the user can receive incoming calls from other xpressa phones in the same network, but cannot receive calls from xpressa phones on the other side of a firewall, that firewall and xpressa phone may not be properly configured. See Working with firewalls and NAT on page 94.

Problems with outgoing calls

If an xpressa phone can receive calls, but cannot make outgoing calls:

- Check the network connection as described on page 122.
- Validate the phone’s address as described on page 122.

Additional procedures follow.

Check firewall configuration

If the user is trying to call through a firewall, make sure that both the firewall and the destination phone are configured to receive calls. See Working with firewalls and NAT on page 94.

Verify call authentication settings

The user may be attempting to call a destination that accepts only calls made by previously authorized users. See Setting up authentication for outgoing calls on page 89 for information on authorizing outgoing calls.

Check dial plan and digit map parameters

When making peer-to-peer calls, if the PHONESET_DIALPLAN_LENGTH parameter is set to a value greater than the length of your extension num-
Troubleshooting

When an outgoing call fails the xpressa phone retains the JTAPI error code and, if available, the SIP response code received. Users can view these codes and explanatory text by pressing the Info button on the call’s status screen or in the Call Log.

For more information on these codes, refer to the documentation available at http://java.sun.com/products/jtapi/ for JTAPI error codes. Request for Comments 2543 describes standard SIP status code definitions; Internet Draft draft-ietf-sip-rfc2543bis-05.txt lists additional codes.

One-way conversation

If audio is flowing only one way, either to or from an xpressa phone:

• Adjust the volume as described on page 121.
Support checklists

- Compare handset and speakerphone as described on page 120.
- Check firewall configuration as described on page 123.
Additional procedures follow.

Check network settings

Follow the procedure described on page 22 to verify the xpressa phone’s current network settings.

Use the SIP message log

Produce a record of the SIP messages sent and received by the xpressa phone with the SIP message log. This log is described on page 128.

No access to browser-based interface

Check the phone’s power (page 119) and network connection (page 122). Additional procedures follow. These procedures may also be useful if a user reports difficulty accessing the MyPingtel user portal.

Verify the URL

To access the phone’s browser-based interface, make sure that the user enters the correct URL for the phone’s embedded web server:
- Verify the IP address for the xpressa phone.
- Find out if the port number is set to a value other than 80. See page 63.
- Verify the format used for the URL: http://<phone IP address> or http://<phone IP address>:<port number>.

Check the myxpressa Web setting

Make sure that the phone’s embedded web server is running. See Controlling browser access on page 63 for more information.
Troubleshooting

Verify the user name and password
All users must supply a user name and password to access the browser-based interface as described on page 44. Work with the xpressa phone’s user to make sure that identifiers are defined and supplied correctly.

For the MyPingtel user portal, users choose their own user names and passwords when they register.

Connection is noisy
Compare handset and speakerphone as described on page 120. An additional procedure follows.

Eliminate radio interference
In a domestic environment, xpressa phones may cause or be affected by radio interference. Turn off other devices while the xpressa phone is in use.

xpression applications don't load or run
To install an xpression application, a user installs a reference to the application’s .JAR file on an external web site or local web server. Installed xpression applications load dynamically each time the xpressa phone restarts.

Check the connection
If an xpression application does not load or does not appear on the Apps tab, check the network connection to the source location. If the connection is down, the xpression application will not be available.

Check the URL
If an xpression application installs successfully, but later does not load or appear on the Apps tab, the .JAR file may have been renamed or relocated
at its host web site. Verify the URL for the xpression application’s .JAR file. If it has changed, uninstall the old location and then install the correct URL.

**Physical defects**

If there is a physical or mechanical problem with an xpressa phone, refer to the warranty card enclosed with the xpressa phone.

For defective equipment replacement procedures, please check the warranty information on Pingtel’s web site at http://support.pingtel.com/, send e-mail to support@pingtel.com or call the Technical Assistance Center at 1-800-PINGTEL (1-800-746-4835).

When you send e-mail or call, please provide the hardware model number, serial number (MAC address), and REV manufacturing code that appear on the label on the bottom of the xpressa phone.
Troubleshooting tools

To help you detect problems, Pingtel offers:

- A logging utility that records SIP messages. See page 141.
- A console output option for debugging activities. See page 142.
- An upgrade log that automatically tracks changes to an xpressa phone’s software. See page 142.
- A file list that helps you review the files stored on an xpressa phone. See page 143.

You use the phone’s browser-based interface to work with these tools.

Using the SIP message log

The SIP logging utility stores all of the SIP messages sent and received by an xpressa phone in a chronological log. This log can help you identify the causes of xpressa phone problems when outgoing calls cannot be completed. Four examples follow on page 130.

You use the browser-based interface to log SIP messages and review the contents of this log.

For background information on SIP and a sample message see page 148.

To log SIP messages

   For information on accessing the myxpressa home page, see page 26.
   A form with buttons to enable and disable the SIP log opens.

2. To begin logging all SIP messages, click Enable Sip Logging. This action:
   - Deletes the log’s previous contents (if any).
   - Logs all SIP messages sent and received by the xpressa phone until
you disable this feature.

3 To review the SIP messages in the log, click **Reload Sip Log**. The web page refreshes to display the log.

Reviewing the log’s contents does not interrupt the logging process. The log adds new messages continuously. When the log reaches 100KB in size, the oldest messages are deleted automatically.

To stop logging SIP messages, click **Disable Sip Logging**.

**Tip** Do not use your browser’s Reload button on this web page. Doing so toggles the Enable/Disable button.

**To review the SIP log**

Complete SIP messages display in the SIP log. The SIP logging utility adds a line of descriptive text to the beginning of each message, and inserts a separator at the end of each message.

<table>
<thead>
<tr>
<th>Message separator</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>=-=-=-=END=-=-=-=</td>
<td>The end of a request sent by a Pingtel phone.</td>
</tr>
<tr>
<td>=-=-=-=END=-=-=-=</td>
<td>The end of an unparsed response received by a</td>
</tr>
<tr>
<td></td>
<td>Pingtel phone.</td>
</tr>
<tr>
<td>++++++++END+++++++</td>
<td>The end of a parsed response received by a Pingtel phone, or a failed message sent by a Pingtel phone.</td>
</tr>
</tbody>
</table>

The SIP log records both the unparsed and the literal, parsed version of the messages received by the phone. Comparing these versions may help you pinpoint a problem with an xpressa phone.

**Tip** Due to the multithreaded nature of the xpressa phone’s platform, logged messages may appear in a different sequence than they were actually sent or received.
Troubleshooting

Example 1: Destination address cannot be resolved

If an outgoing call fails immediately, it may indicate a problem with the destination address. The SIP log can help you determine if the DNS server cannot resolve the destination address.

The SIP log that follows shows just one request, and includes the description **ERROR: UDP SIP User Agent failed to send message.** This indicates that the SIP user agent has encountered an immediate error and there is no attempt to resend the request. Possible causes of this problem include:

- The xpressa phone is not connected to the network.
- The SIP URL contains an invalid DNS host name.
- The user dials digits to make the call, but either the **SIP_DIRECTORY_SERVERS** parameter is not defined or no matching dial plan is defined by the **PHONESET_DIGITMAP** parameter.
- The DNS server may be configured with an incorrect address.

Enable the phone’s SIP log and try making the call again in an identical manner. Compare the contents of the SIP log to the example that follows.
Example 2: Addressee does not support SIP

The messaging pattern in this SIP log shows the messages sent when a legitimate address is dialed, but that destination either does not exist or is not currently configured to listen for SIP. For example, the address might correctly identify an instant xpressa softphone on a PC, but if the softphone is not running, sending SIP messages to it will result in an error.

The sequence of the messages in this log shows that the request is sent via UDP twice, then via TCP once before the error is received. This pattern is characteristic of UDP, which is datagram-based and cannot respond immediately when an error occurs.
Troubleshooting

Tip In this example, "..." indicates data identical to that shown in the first message in the log.

SIP Message Log

UDP SIP User Agent sent message:  
INVITE sip:10.1.1.111:222 SIP/2.0  
From: sip:58@10.1.1.58;tag=1c12837  
To: sip:10.1.1.111:222  
Call-Id: call-98460315-20@10.1.1.58  
Cseq: 1 INVITE  
Content-Type: application/sdp  
Content-Length: 194  
Accept-Language: en  
Supported: sip-cc, sip-cc-01, timer  
Contact: sip:58@10.1.1.58  
User-Agent: Pingtel/0.9.0 (VxWorks)  
Via: SIP/2.0/UDP 10.1.1.58  
v=0  
o=Pingtel 5 5 IN IP4 10.1.1.58  
s=phone-call  
t=IN IP4 10.1.1.58  
t=0 0  
m=audio 8766 RTP/AVP 0 96 8  
a=rtpmap: 0 pcmu/8000/1  
a=rtpmap: 96 telephone-event/8000/1  
a=rtpmap: 8 pcma/8000/1  
-----------------END------------------  
resend 1 of UDP message  
ERROR: UDP SIP User Agent failed to send message:  
INVITE sip:10.1.1.111:222 SIP/2.0  
...  
-----------------END------------------  
ERROR: TCP SIP User Agent failed to send message:  
INVITE sip:10.1.1.111:222 SIP/2.0  
TCP message  
...  
-----------------END------------------  
SIP User agent FAILED to send message:  
INVITE sip:10.1.1.111:222 SIP/2.0  
error message  
...  
++++++++++++++++++++END+++++++++++++++++++

2nd UDP message

3rd UDP message

TCP message
Example 3: Call not getting through to destination

The SIP log in this example shows the messages sent by an xpressa phone when there is no response from a valid destination address. The message is sent via UDP a total of seven times, then sent once via TCP before the call finally fails.

This situation may occur, for example, if the destination is on the other side of a firewall: the xpressa phone sends requests, but cannot receive a response unless the firewall and both user agents are configured correctly.

Tip In this example, "..." indicates data identical to that in the first message.

SIP Message Log

UDP SIP User Agent sent message:  
INVITE sip:10.1.1.58:222 SIP/2.0  
From: sip:107@10.1.1.111;tag=1c41  
To: sip:10.1.1.58:222  
Call-Id: call-984598853-4@10.1.1.111  
Cseq: 1 INVITE  
Content-Type: application/sdp  
Content-Length: 196  
Accept-Language: en  
Supported: sip-cc, sip-cc-01, timer  
Contact: sip:107@10.1.1.111  
User-Agent: Pingtel/0.9.0 (WinNT)  
Via: SIP/2.0/UDP 10.1.1.111  
v=0  
o=Pingtel 5 5 IN IP4 10.1.1.111  
s=phone-call  
c=IN IP4 10.1.1.111  
t=0 0  
m=audio 8766 RTP/AVP 0 96 8  
a=rtpmap: 0 pcmu/8000/1  
a=rtpmap: 96 telephone-event/8000/1  
------------------------END-------------------
**Troubleshooting**

resend 1 of UDP message
UDP SIP User Agent sent message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
------------------------END------------------------
resend 2 of UDP message
UDP SIP User Agent sent message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
------------------------END------------------------
resend 3 of UDP message
UDP SIP User Agent sent message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
------------------------END------------------------
resend 4 of UDP message
UDP SIP User Agent sent message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
------------------------END------------------------
resend 5 of UDP message
UDP SIP User Agent sent message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
------------------------END------------------------
resend 6 of UDP message
UDP SIP User Agent sent message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
------------------------END------------------------
ERROR: TCP SIP User Agent failed to send message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
------------------------END------------------------
SIP User agent FAILED to send message:
INVITE sip:10.1.1.58:222 SIP/2.0
...
++++++++++++++++++++END++++++++++++++++++++
Example 4: Multiple responses to the same request

This example shows a log with duplicate responses, rather than the duplicate requests shown in the previous examples. This demonstrates an inability between the participants in a call to correctly associate responses with requests.

The first request in this example is an INVITE. The response is an authentication challenge from a Proxy server. A second INVITE is then sent with the authentication data. Note that the Cseq value changes from 1 INVITE to 2 INVITE to identify these different SIP transactions.

After the call is set up, it begins to show duplicate responses. Review the values in the To, From, and Cseq fields in a SIP response: these values should match the values in the original request.

Tip To compare the To and From fields, the user ID, host address, port (if specified), and tag must match exactly. However, requests do not include a tag in the To field, although responses do include tags.

While a single duplicate response may be sent when the network is slow, more than one duplicate indicates a more serious problem. In most cases, a message log like this results only from a software error or incompatibility.
Troubleshooting

SIP Message Log

UDP SIP User Agent sent message:

INVITE sip:87681435@216.124.44.28 SIP/2.0
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:87681435@216.124.44.28
Call-Id: call-984512430-12@116.214.41.73
Cseq: 1 INVITE
Content-Type: application/sdp
Accept-Language: en
Supported: sip-cc, sip-cc-01, timer
Contact: sip:7683291@116.214.41.73
User-Agent: Pingtel/0.9.0 (VxWorks)
Via: SIP/2.0/UDP 116.214.41.73

v=0
c=IN IP4 116.214.41.73
m=audio 8766 RTP/AVP 0 96 8
a=rtpmap: 0 pcmu/8000/1
a=rtpmap: 96 telephone-event/8000/1
a=rtpmap: 8 pcma/8000/1

-------------------END-------------------
Read SIP message:

```
SIP/2.0 407 Proxy Authentication Required
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:87681435@216.124.44.28;tag=2b000286
Call-ID: call-984512430-12@116.214.41.73
CSeq: 1 INVITE
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
Proxy-Authenticate: DIGEST
realm="REALM",nonce="a1f996feacc29e56080086cbb2e99409"
CID: call-984512430-12@116.214.41.73
```

SIP/2.0 407 Proxy Authentication Required
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:87681435@216.124.44.28;tag=2b000286
Call-ID: call-984512430-12@116.214.41.73
CSeq: 1 INVITE
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
Proxy-Authenticate: DIGEST
realm="REALM",nonce="a1f996feacc29e56080086cbb2e99409"
CID: call-984512430-12@116.214.41.73

UDP SIP User Agent sent message:

```
ACK sip:87681435@216.124.44.28;tag=2b000286 SIP/2.0
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:87681435@216.124.44.28;tag=2b000286
Call-ID: call-984512430-12@116.214.41.73
Cseq: 1 ACK
Accept-Language: en
User-Agent: Pingtel/0.9.0 (VxWorks)
Via: SIP/2.0/UDP 116.214.41.73
```

--------- unparsed response
--------- parsed response
--------- unparsed response
--------- parsed response
--------- ACK sent
Troubleshooting

UDP SIP User Agent sent message:
INVITE sip:87681435@216.124.44.28 SIP/2.0
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:87681435@216.124.44.28
Call-Id: call-984512430-126116.214.41.73
Cseq: 2 INVITE
Content-Type: application/sdp
Accept-Language: en
Supported: sip-cc, sip-cc-01, timer
Contact: sip:7683291@116.214.41.73
User-Agent: Pingtel/0.9.0 (VxWorks)
Proxy-Authorization: DIGEST
USERNAME="*24#87654321", REALM="REALM",
NONCE="a1f996feacc29e56080086cbb2e99409",
RESPONSE="b721c8bb7ffe554e2ce1dc37863b0805",
URI="sip:87681435@216.124.44.28"
Via: SIP/2.0/UDP 116.214.41.73

v=0
o=Pingtel 5 5 IN IP4 116.214.41.73
s=phone-call
c=IN IP4 116.214.41.73
t=0 0
m=audio 8766 RTP/AVP 0 96 8
a=rtpmap: 0 pcmu/8000/1
a=rtpmap: 96 telephone-event/8000/1
a=rtpmap: 8 pcma/8000/1

Read SIP message:
SIP/2.0 100 Trying
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:7683291@216.124.44.28
Call-ID: call-984512430-126116.214.41.73
CSeq: 2 INVITE

2nd INVITE with authentication credentials

unparsed TRYING response

--------------------END--------------------

Read SIP message:
SIP/2.0 100 Trying
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:7683291@216.124.44.28
Call-ID: call-984512430-126116.214.41.73
CSeq: 2 INVITE

unparsed TRYING response

--------------------END--------------------
Troubleshooting tools

SIP/2.0 100 Trying
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:876814358216.124.44.28
Call-Id: call-984512430-12@116.214.41.73
Cseq: 2 INVITE
...

 невозможность END

Read SIP message:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:876814358216.124.44.28;tag=c294300013445c0-0
Call-ID: call-984512430-12@116.214.41.73
Cseq: 2 INVITE
...

 невозможно END

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:876814358216.124.44.28;tag=c294300013445c0-0
Call-ID: call-984512430-12@116.214.41.73
Cseq: 2 INVITE
...

 невозможность END

Read SIP message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:7683291@216.124.44.28;tag=1c11408
To: sip:876814358216.124.44.28;tag=c294300013445c0-0
Call-ID: call-984512430-12@116.214.41.73
Cseq: 2 INVITE
Content-Type: application/sdp
...

 невозможность END
Troubleshooting

SIP/2.0 200 OK
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:7681291@216.124.44.28;tag=1c11408
To: sip:7681291@216.124.44.28;tag=1c11408
Call-ID: call-984512430-12@116.214.41.73
Cseq: 2 INVITE
Content-Type: application/sdp
...

 UDP SIP User Agent sent message:
ACK sip:7681291@216.124.44.28 SIP/2.0
From: sip:7681291@216.124.44.28;tag=1c11408
To: sip:7681291@216.124.44.28;tag=1c11408
Call-ID: call-984512430-12@116.214.41.73
Cseq: 2 ACK
...

Read SIP message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:7681291@216.124.44.28;tag=1c11408
To: sip:7681291@216.124.44.28;tag=1c11408
Call-ID: call-984512430-12@116.214.41.73
Cseq: 2 INVITE
...

Received duplicate message
SIP/2.0 200 OK
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:7681291@216.124.44.28;tag=1c11408
To: sip:7681291@216.124.44.28;tag=1c11408
Call-ID: call-984512430-12@116.214.41.73
Cseq: 2 INVITE
Content-Type: application/sdp
...

++++++++++++++++++++END++++++++++++++++++++
Setting configuration parameters for troubleshooting

To show the output of debugging activities on a console, you set one or both of the following parameters.

**ALLOW_CONSOLE_OUTPUT**

To retrieve console logs for troubleshooting or other support activities, you set the **ALLOW_CONSOLE_OUTPUT** parameter to ENABLE on the affected phone. This parameter is stored in the user-config file. Removing this parameter or the value ENABLE prevents console output from being produced.

You use the browser-based interface described on page 26 to add or remove this parameter. In the browser-based interface, click **Administration: Phone Configuration** then scroll to the Additional Parameters text box at the bottom of this page.

---

**Troubleshooting tools**

---

Read SIP message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:768814350216.124.44.28;tag=1c11408
To: sip:768814350216.124.44.28;tag=c294300013445c0-0
Call-ID: call-984512430-12@116.214.41.73
CSeq: 2 INVITE
...

Received duplicate message
SIP/2.0 200 OK
Via: SIP/2.0/UDP 116.214.41.73;received=116.214.41.73
From: sip:768814350216.124.44.28;tag=1c11408
To: sip:768814350216.124.44.28;tag=c294300013445c0-0
Call-ID: call-984512430-12@116.214.41.73
CSeq: 2 INVITE
Content-Type: application/sdp
...

3rd OK unparsed

3rd OK parsed
Troubleshooting

JAVA_OUTPUTSTREAM_REDIRECT

To produce Java debugging output, you set values for two parameters:
ALLOW_CONSOLE_OUTPUT : ENABLE
JAVA_OUTPUTSTREAM_REDIRECT : CONSOLE

The JAVA_OUTPUTSTREAM_REDIRECT parameter is stored in the user-config file. Both parameters must be present and set to the values shown for output to be produced.

You use the browser-based interface described on page 26 to add or remove this parameter. In the browser-based interface, click Administration: Phone Configuration then scroll to the Additional Parameters text box at the bottom of this page.

Using the upgrade log

An upgrade log automatically records all manual software upgrades performed on an xpressa phone. Upgrades made using the VersionCheck xpression application do not appear in this log.
To review this log, on the myxpressa home page click **Administration: Upgrade Log**. The log displays upgrade steps chronologically. An example follows.

**Tip** For information on accessing the myxpressa home page, see page 26.

**Reviewing the file list**

You can review a list of the files stored on an xpressa phone. This list provides file sizes, which can help you verify the cause of space or memory-related problems.

To review an xpressa phone’s file list, on the myxpressa home page click **Administration: File Listing**.

For information on accessing the myxpressa home page, see page 26.
Troubleshooting

An example follows.

Review configuration files

The xpressa phone stores all defined configuration parameters and values in two ASCII text files: **pinger-config** and **user-config**. In addition, xpressa phones store all installed xpression applications in the **app-config** ASCII text file. To investigate a problem it may be useful to review the exact contents of these text files.

**What to look for in manually edited files**

If you modify the **pinger-config** and **user-config** files manually as described on page 29, instead of using the phonetop or browser-based interfaces, you may introduce values with incorrect syntax or other irregularities that cannot be parsed.
If you suspect that such problems exist in your configuration files:

- Review the parameter : value format information on page 29.
- Compare your files to the default files shown on page 35 to make sure that they are valid.
- Revise files to remove any extraneous line feeds (carriage returns) or characters, particularly colon (:) characters.

In addition, remember that if values are stored in both files for the same parameter, the value stored in the user-config file overrides the value stored in the pinger-config file.

If you edit the app-config file manually, be sure to:

- Start each line with \texttt{USER}, and a space before you supply the URL.
- Start comment lines with the \# character.

See page 111 for information on \textit{Editing an app-config file}.

\textbf{Note} The instant xpressa softphone is limited to a maximum of five xpression applications, including standard, supplied applications.

\textbf{Printing a configuration file}

To facilitate analysis, you can print the contents of an xpressa phone’s configuration files. Follow the procedures for \textit{Editing configuration files manually} on page 29 and use your ASCII text editor to print the file.

\textbf{Contact Pingtel's TAC}

Before you contact Pingtel’s Technical Assistance Center, please be prepared to provide:

- Hardware model number, REV manufacturing code, and serial number (MAC address) for xpressa phones.
- Serial number (instant xpressa softphone).
Troubleshooting

- Software version number.

In addition, please use Pingtel's Support services as described on page 10.

To contact Pingtel's Technical Assistance Center (TAC):
- Send e-mail to support@pingtel.com.
- Call the TAC at 1-800-PINGTEL (1-800-746-4835) from within the US.
- Call the TAC at (781) 938-5306 from outside the US.
FCC information

The xpressa phone appliance has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

The xpressa phone appliance generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this instruction manual, may cause harmful interference to radio communications. Operation of an xpressa phone in a residential area is likely to cause harmful interference. In such a case, users will be required to correct the interference at his or her own expense.

WARNING

The xpressa phone is a Class A product. In a domestic environment this product may cause radio interference, which may require users to take adequate measures.

Caution

Changes or modifications to an xpressa phone that are not expressly approved by the manufacturer may void your FCC granted authority to operate the equipment.

Caution

After certain electrostatic discharge (ESD) events, you may need to restart the xpressa phone manually. The xpressa phone offers a manual reset switch, located on the bottom of the phone, to restart the phone. See page 113.
Appendix A: Session Initiation Protocol

The Session Initiation Protocol (SIP) establishes a standard methodology for setting up, maintaining, and ending interactive communication sessions. To perform these tasks SIP, like HTTP (HyperText Transfer Protocol), uses a request-response model in which messages are exchanged by system components.

The particular content of a session is described in, but not included with, SIP messages. Pingtel's xpressa phones use SIP to manage the transmission of voice data during phone calls, but SIP can also be used for the transmission of other types of data, such as video, fax, and multimedia.

Tip SIP messages may actually travel over different networks than the audio or video packets they describe.

This section introduces the contents of SIP messages and describes how the messages are organized into transactions, sessions, and calls. For information on setting up your SIP environment see page 71.

The Internet Engineering Task Force (IETF) Request for Comments (RFC) 2543 provides the specification for the SIP protocol.

SIP messages

SIP is ASCII-based: all SIP messages are formatted as text using HTTP syntax. Messages contain call control methods for requests or response codes for replies, and are exchanged to:

- Initiate a session between an originator and a target. This involves:
  - locating the target
  - determining whether or not the target is available
  - determining the media capabilities of the target
Establish a connection between the originator and the target
End the session by terminating or transferring the connection

Descriptions of the SIP methods and response codes, the required fields in SIP message headers, SIP URLs, and examples of SIP messages and message flows follow.

**Methods**

SIP call control methods identify the type of request that is being made:

<table>
<thead>
<tr>
<th>Method</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>Invites a target to participate in a session; establishes a connection. Also used to change call state or capabilities, such as the codec used.</td>
</tr>
<tr>
<td>ACK</td>
<td>Confirms receipt of a final response to an INVITE request.</td>
</tr>
<tr>
<td>BYE</td>
<td>Indicates that either the originator or the target wishes to end the call; terminates a connection or declines an invitation.</td>
</tr>
<tr>
<td>REFER</td>
<td>Indicates that the recipient should contact a third party using provided contact information; initiates a transfer.</td>
</tr>
<tr>
<td>CANCEL</td>
<td>Cancels a pending request; does not affect a completed request.</td>
</tr>
<tr>
<td>REGISTER</td>
<td>Registers a user’s address with a SIP location server; resolves a public address to a specific address. Not related to specific session.</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>Solicits information about features supported by SIP servers such as supported methods and media capabilities.</td>
</tr>
<tr>
<td>NOTIFY</td>
<td>Provides information about a state change; not related to a specific session. Used for message waiting communications with a voice mail server and to indicate the outcome of transfers.</td>
</tr>
<tr>
<td>SUBSCRIBE</td>
<td>Indicates the desire for NOTIFY (state change) requests. Used for message waiting communications with a voice mail server.</td>
</tr>
</tbody>
</table>
Appendix A: Session Initiation Protocol

xpressa phones support these SIP methods:

<table>
<thead>
<tr>
<th>Methods Initiated</th>
<th>Methods Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITE</td>
<td>INVITE</td>
</tr>
<tr>
<td>ACK</td>
<td>ACK</td>
</tr>
<tr>
<td>BYE</td>
<td>BYE</td>
</tr>
<tr>
<td>REFER</td>
<td>REFER</td>
</tr>
<tr>
<td>CANCEL</td>
<td>CANCEL</td>
</tr>
<tr>
<td>REGISTER</td>
<td></td>
</tr>
<tr>
<td>OPTIONS</td>
<td>OPTIONS</td>
</tr>
<tr>
<td>NOTIFY</td>
<td>NOTIFY</td>
</tr>
<tr>
<td>SUBSCRIBE</td>
<td></td>
</tr>
</tbody>
</table>

Response codes

SIP response codes indicate the status of a session. Response codes are generated and sent in outgoing messages, and accepted when received in incoming messages.

<table>
<thead>
<tr>
<th>Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1xx</td>
<td>Informational: trying, ringing, forwarding, queuing, in progress</td>
</tr>
<tr>
<td>2xx</td>
<td>Successful: Ok</td>
</tr>
<tr>
<td>3xx</td>
<td>Redirection: indicate additional information for call forwarding</td>
</tr>
<tr>
<td>4xx</td>
<td>Request Failure: indicate request errors such as missing information</td>
</tr>
<tr>
<td>5xx</td>
<td>Server Failure: time outs, unavailable services, and other server errors</td>
</tr>
<tr>
<td>6xx</td>
<td>Global Failures: busy, declined, not found, not acceptable</td>
</tr>
</tbody>
</table>
Responses with a 1xx response code are also called provisional responses, while the remaining response codes (2xx, 3xx, 4xx, 5xx, and 6xx) indicate final responses.

Refer to Request for Comments 2543 for standard SIP status code definitions. Additional codes may also be listed in Internet Draft draft-ietf-sip-rfc2543bis-05.txt.

**Message headers**

Each SIP message is accompanied by a header. The required fields in the message header are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>The address of the session originator, expressed as a SIP URL.</td>
</tr>
<tr>
<td>To</td>
<td>The address of the session target, expressed as a SIP URL.</td>
</tr>
<tr>
<td>Call-ID</td>
<td>A unique identifier assigned to all of the SIP messages related to a call.</td>
</tr>
<tr>
<td>Cseq</td>
<td>The SIP call control method and an identifying sequence number.</td>
</tr>
</tbody>
</table>

**Sample SIP message**

Here’s an example of the SIP message that is sent when one xpressa phone dials another:
Appendix A: Session Initiation Protocol

Request Method

```plaintext
INVITE sip:10.1.1.56 SIP/2.0
From: sip:Lucille@10.1.1.58;tag=1c6227
To: sip:10.1.1.56
Call-Id: call-973007935-1@10.1.1.58
Cseq: 1 INVITE
Content-Type: application/sdp
Content-Length: 104
Accept-Language: en
Supported: sip-cc, sip-cc-01, timer
Contact: sip:Lucille@10.1.1.58
User-Agent: Pingtel/0.7.0 (VXWorks)
Via: SIP/2.0/UDP 10.1.1.58
v=0
c=Pingtel 5 5 IN IP4 10.1.1.58
s=phone-call
c=IN IP4 10.1.1.58
t=0 0
m=audio 8766 RTP/AVP 0 8
```

Message flow examples

To illustrate the sequence and direction in which SIP call control methods and response codes are sent, message flow examples follow for:

- Call setup
- Call tear down
- Successful transfer (blind)
- Successful transfer (consultative)
### Call setup

**Caller**

- Invite method sent
- ACK method sent

**Callee**

- 100 Trying response code sent
- 180 Ringing response code sent
- 200 Ok response code sent

### Call teardown

**Caller**

- Invite method sent
- BYE method sent

**Callee**

- 200 Ok response code sent

### Successful blind transfer

<table>
<thead>
<tr>
<th>Xfer Controller</th>
<th>Transferee</th>
<th>Xfer Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Invite sent</td>
<td></td>
</tr>
<tr>
<td>200 Ok sent</td>
<td>ACK sent</td>
<td>200 Ok sent</td>
</tr>
<tr>
<td>[Controller presses TRANSFER and dials Target]</td>
<td>Invite (hold) sent</td>
<td>200 Ok (to INVITE)</td>
</tr>
<tr>
<td></td>
<td>ACK sent</td>
<td>202 Accepted (to REFER)</td>
</tr>
<tr>
<td></td>
<td>REFER sent</td>
<td>[Consultative call]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[Target answers]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>200 Ok sent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACK sent</td>
</tr>
<tr>
<td></td>
<td>NOTIFY (transfer complete)</td>
<td>NOTIFY (transfer complete)</td>
</tr>
<tr>
<td>200 Ok (to NOTIFY)</td>
<td>BYE sent</td>
<td>200 Ok (to BYE)</td>
</tr>
</tbody>
</table>

[Target hangs up]
Appendix A: Session Initiation Protocol

**Successful consultative transfer**

<table>
<thead>
<tr>
<th>Xfer Controller</th>
<th>Transferee</th>
<th>Xfer Target</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>200 Ok (to BYE)</td>
</tr>
<tr>
<td>INVITE sent</td>
<td>ACK sent</td>
<td></td>
</tr>
<tr>
<td>[Controller presses TRANSFER and dials Target]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVITE (hold)</td>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>ACK sent</td>
<td>INVITE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 Ok (to INVITE)</td>
<td></td>
</tr>
<tr>
<td>[Target answers]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td>INVITE</td>
<td></td>
</tr>
<tr>
<td>Controller presses Transfer or hangs up:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INVITE (hold)</td>
<td>ACK</td>
<td></td>
</tr>
<tr>
<td>ACK</td>
<td>REFER</td>
<td></td>
</tr>
<tr>
<td>REFERENCES sent with Replace header field in Target URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>202 Accepted (to REFER)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>INVITE sent with Replace header</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACK sent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 Ok sent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BYE sent</td>
<td></td>
</tr>
<tr>
<td>200 Ok (to BYE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[Connection made between transferee and target]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOTIFY (transfer)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 Ok (to NOTIFY)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SIP addresses

SIP URLs use the same format as IP addresses or e-mail addresses:

Display Name<sip:user-id@server-address:port;parameters;?header-names=values>

The formats of some sample SIP URLs might appear as:

- sip:123@pingtel.com
- sip:4444@10.1.1.123
- sip:freds@sip.pingtel.net:5070
- Fred Smith<sip:freds@sip.pingtel.net:5070>

Instead of being assigned to specific devices the way that telephone numbers traditionally are assigned, SIP URLs are assigned to the individual users who participate in SIP sessions. As a result, when a phone call (or other interactive session) is made to a SIP address, it can be routed to the appropriate individual regardless of a change in physical location or IP telephone device.

The From and To fields in every SIP message header contain the SIP URLs of the session’s originator and target.

SIP transactions

A SIP transaction consists of a set of related SIP messages: usually, a request such as an INVITE, zero or more provisional responses (1xx response code), and a final response (2xx or greater). For example, the set of messages sent by a callee phone during call setup to indicate trying,
Appendix A: Session Initiation Protocol

ringing, and Ok make up a SIP transaction. See page 152 for an example of this message flow.

The message header To, From, Call-ID, and Cseq fields have the same values in every message in a SIP transaction.

SIP sessions

SIP sessions encompass all messages sent between two SIP endpoints. That is, all SIP messages sent between two phones, beginning with call setup and ending with call teardown, make up a SIP session.

The headers of all messages involved in a SIP session have the same values in the To, From, and Call-ID fields; however, the addresses in the To and From fields switch to reflect the phone that originated the message.

SIP calls

A SIP call consists of one or more sessions. An example of a call that encompasses multiple sessions is a conference call.

All SIP messages in a call will have the same values in all Call-ID message header fields.

System components

Components in a SIP system send and respond to the messages that set up, establish, and terminate sessions.

Tip SIP components are abstractions: they do not have a one-to-one correspondence to specific VoIP devices.
System components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAC (User Agent Client)</td>
<td>An application that initiates a request and sends it in a SIP message.</td>
</tr>
<tr>
<td>UAS (User Agent Server)</td>
<td>An application that uses a SIP message to respond to a request; accepts, redirects, or refuses sessions.</td>
</tr>
<tr>
<td>Proxy server</td>
<td>An intermediary program that accepts a SIP message, optionally performs services, and then passes the message on.Acts as both a UAC and a UAS.</td>
</tr>
<tr>
<td>Redirect server</td>
<td>An intermediary program that accepts a SIP message and then returns a response to the sender. A Redirect server may or may not perform services.</td>
</tr>
<tr>
<td>Registry server</td>
<td>A server that accepts SIP messages from, and registers the current location of, a user agent. Maintains a database of addresses for user agents.</td>
</tr>
<tr>
<td>Location server</td>
<td>A server that provides information to Redirect and Proxy servers about the possible locations of a session target.</td>
</tr>
</tbody>
</table>

Generally,

- User agents are the peers in the VoIP peer-to-peer communication model.
- Proxy servers monitor sessions and provide services.
- Redirect, Registry, and Location servers support user mobility by tracking the location of, and redirecting messages to, session targets.

For more information on setting up a SIP environment for xpressa phones see page 71.
Appendix A: Session Initiation Protocol

Supported SIP features

For reference, a list of the SIP capabilities and features supported by xpressa phones follows.

- Basic call setup
- Bridged conferencing
- Hold and off hold
- Transfer:
  - Consultative transfer: REFER and Replaces, as described by Internet Drafts draft-ietf-sip-cc-transfer-04.txt and draft-biggs-sip-replaces-00.txt
  - Blind transfer: REFER, as described by Internet Draft draft-ietf-sip-cc-transfer-04.txt
  - Blind transfer: BYE Also (if REFER fails or is unsupported), as described by expired Internet Draft draft-ietf-mmusic-cc-01.txt
- Early media (SDP in 180/183)
- Delayed SDP (SDP in ACK)
- Session timer, as described in the IETF Internet Draft draft-ietf-sip-session-timer-04.txt
- Re-INVITE: codec change, hold, off-hold, session timer
- Forwarding (302 redirect): forward on busy, unconditional forward, and forward on no answer
- REGISTER with refresh
- UDP/TCP
- Supported header field
- Route/Record-Route header fields
Supported SIP features

- Basic and Digest incoming Authentication, Proxy Authentication, and outgoing Authentication
- Public and private IP Address support for use with NAT firewalls
- Configurable SIP and RTP/RTCP ports
- RTP codecs 0, 8 (G.711 a-law, u-law)
- Out-of-band DTMF (DTMF over RTP) in compliance with RFC 2833
- Voice mail status messaging, as described by Internet Draft draft-mahy-sip-message-waiting-02.txt
Appendix B: Parameter reference

For reference, this appendix provides a brief description of every configuration parameter and provides:
• The default value for parameters that have a supplied default.
• Data entry options, including all valid values if a limited set is available.
• The minimum and maximum for the number of times you can add this parameter and a value.
  • The minimum is either 0 (for parameters that are not required) or 1 (for required parameters).
  • The maximum is either 1 or unlimited. For unlimited parameters, you enter each parameter : value on an individual line.
• Where the parameter can be set: on the phonetop, through a browser, or both, and the configuration file in which it is stored.
• Who can change a configuration setting: the admin or any user.

For more information, see Configuring an xpressa phone on page 24. Click on any parameter name for detailed information on that parameter or see the descriptions that begin on page 46.

**Dialing**

**PHONESET_EXTENSION : <extension>**

The unique identifier for an xpressa phone.

- **Default:** 4444
- **Options:** Alphanumeric
- **Min/max:** 1/1
- **Examples:**
  - PHONESET_EXTENSION : Sales
  - PHONESET_EXTENSION : 207
**PHONESET_EXTENSION** : <extension>

**Interface:**
Browser — Administration: Phone Configuration  
File — pinger-config  

**Access:**  
Admin only

**PHONESET_DIALPLAN_LENGTH** : <length>

The length of the phone numbers most frequently dialed from this xpressa phone.

- **Default:** 4  
- **Options:** Numeric; must be greater than or equal to 2  
- **Min/max:** 1/1  
- **Example:** 

```
PHONESET_DIALPLAN_LENGTH : 3
```

**Interface:**
Browser — Administration: Phone Configuration  
File — pinger-config  

**Access:**  
Admin only

**PHONESET_DIGITMAP**.<dial plan> : <routing address>

Stores dial plans and their routing addresses to automate dialing.

- **Default:** N/A  
- **Options:** Alphanumeric dial plan and alphanumeric SIP URL  
  A null address uses the defined SIP Directory server's address  
- **Min/max:** 0/unlimited  
- **Examples:** 

```
PHONESET_DIGITMAP.xxx :
PHONESET_DIGITMAP.0 : sip:info@mycompany.com
```

**Interface:**
Browser — Administration: Phone Configuration  
File — user-config  

**Access:**  
Admin only
Appendix B: Parameter reference

Phone security

**PHONESET_HTTP_AUTH_DB.<user_name> : <password>**

Stores a user name and encrypted password to allow use of the browser-based interface or, if the MyPingtel sign-in application is used, the MyPingtel user portal.

**Default:**
admin : cc3779c1114ba5fd9882afdc7ef267e3

**Options:**
User name — Any alphanumeric value
Password — Any alphanumeric value
Should be entered through the browser-based interface or the MyPingtel sign-in application for proper encryption.

**Min/max:**
1/unlimited

**Example:**
PHONESET_HTTP_AUTH_DB.AMH : caeb7cc31f (etc.)

**Interface:**
Access:
- For the browser-based interface:
  - Only administrators can change the *admin* password on the phone with Prefs: User Maintenance, or set up new users through the browser-based interface with Administration: User Maintenance.
  - All users can change their own passwords in the browser-based interface with Administration: Change Password.

**Interface:**
Access:
- For the MyPingtel user portal:
  - Users register a user name and password for themselves at http://my.pingtel.com, then run the MyPingtel sign-in application on the phonetop to register their phones for this service.
  - MyPingtel sign-in stores the user name and encrypted password when registration is complete.

**PHONESET_TELNET_ACCESS : <access>**

Defines whether to allow Telnet access to this xpressa phone.

**Default:**
DISABLE
Call handling

**PHONESET_TELNET_ACCESS : <access>**

Options: ENABLE or DISABLE
Min/max: 0/1
Example: PHONESET_TELNET_ACCESS : ENABLE
Interface: Browser — Administration: Phone Configuration
File — user-config
Access: Admin only

**PHONESET_RINGER : <method>**

Alert method to use for incoming calls.

Default: BOTH
Options: BOTH, VISUAL, or AUDIBLE
Min/max: 1/1
Example: PHONESET_RINGER : VISUAL
Interface: Phonetop — Prefs: Call Handling
Browser — Preferences: Preferences
MyPingtel — Call Handling
File — user-config
Access: All users

**PHONESET_AVAILABLE_BEHAVIOR : <behavior>**

How the phone directs incoming calls.

Default: RING
Options: RING, FORWARD, or FORWARD_ON_NO_ANSWER
Appendix B: Parameter reference

**PHONESET_AVAILABLE_BEHAVIOR : <behavior>**

- **Min/max:** 1/1
- **Example:** PHONESET_AVAILABLE_BEHAVIOR : FORWARD
- **Interface:**
  - Phonetop — Prefs: Call Handling
  - Browser — Preferences: Preferences
  - MyPingtel — Call Handling
  - File — user-config
- **Access:** All users

**SIP_FORWARD_UNCONDITIONAL : <destination>**

Forwarding destination for all incoming calls (if PHONESET_AVAILABLE_BEHAVIOR = FORWARD).

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Examples:**
  - SIP_FORWARD_UNCONDITIONAL : vm.provider.net
  - SIP_FORWARD_UNCONDITIONAL : 10.1.1.122
- **Interface:**
  - Phonetop — Prefs: Call Handling
  - Browser — Preferences: Preferences
  - MyPingtel — Call Handling
  - File — user-config
- **Access:** All users
SIP_FORWARD_ON_NO_ANSWER : <destination>

Forwarding destination for calls that remain unanswered for
PHONESET_NO_ANSWER_TIMEOUT seconds (if
PHONESET_AVAILABLE_BEHAVIOR = FORWARD_ON_NO_ANSWER).

Default: None
Options: Alphanumeric
Min/max: 0/1
Example: SIP_FORWARD_ON_NO_ANSWER : 17819385306
Interface: Phonetop — Prefs: Call Handling
Browser — Preferences: Preferences
MyPingtel — Call Handling
File — user-config
Access: All users

PHONESET_NO_ANSWER_TIMEOUT : <seconds>

The number of seconds a phone rings before it is considered unanswered. (One
ring is equivalent to six seconds.)

Default: If null, uses 24.
Options: Numeric: multiples of 6
Min/max: 0/1
Example: PHONESET_NO_ANSWER_TIMEOUT : 48
Interface: Phonetop — Prefs: Call Handling
Browser — Preferences: Preferences
MyPingtel — Call Handling
File — user-config
Access: All users
Appendix B: Parameter reference

**PHONESET_CALL_WAITING_BEHAVIOR** : <behavior>

Whether or not to use the call waiting feature.

**Default:** ALERT

**Options:** ALERT or BUSY

**Min/max:** 1/1

**Example:** PHONESET_CALL_WAITING_BEHAVIOR : BUSY

**Interface:**
- Phonetop — Prefs: Call Handling
- Browser — Preferences: Preferences
- MyPingtel — Call Handling
- File — user-config

**Access:** All users

**PHONESET_BUSY_BEHAVIOR** : <behavior>

How to handle incoming calls when the phone is busy and call waiting is not used (that is, PHONESET_CALL_WAITING_BEHAVIOR = BUSY).

**Default:** BUSY

**Options:** BUSY or FORWARD

**Min/max:** 1/1

**Example:** PHONESET_BUSY_BEHAVIOR : FORWARD

**Interface:**
- Phonetop — Prefs: Call Handling
- Browser — Preferences: Preferences
- MyPingtel — Call Handling
- File — user-config

**Access:** All users
**SIP_FORWARD_ON_BUSY** : <destination>

Destination for incoming calls if forwarded when the phone is busy (if PHONESET_CALL_WAITING_BEHAVIOR = BUSY).

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:** SIP_FORWARD_ON_BUSY : voicemail.provider.net
- **Interface:** Phonetop — Prefs: Call Handling
  Browser — Preferences: Preferences
  MyPingtel — Call Handling
  File — user-config
- **Access:** All users

**PHONESET_DND** : <access>

Whether or not to invoke the Do Not Disturb feature for this xpressa phone.

- **Default:** DISABLE
- **Options:** ENABLE or DISABLE
- **Min/max:** 0/1
- **Example:** PHONESET_DND : ENABLE
- **Interface:** Phonetop — Prefs: Call Handling
  Browser — Preferences: Preferences
  MyPingtel — Call Handling
  File — user-config
- **Access:** All users
Appendix B: Parameter reference

**PHONESET_DND_METHOD** : <method>

Result for incoming calls when PHONESET_DND = ENABLE.

- **Default:** FORWARD_ON_BUSY
- **Options:** SEND_BUSY, FORWARD_ON_BUSY, or FORWARD_ON_NO_ANSWER
- **Min/max:** 1/1
- **Example:** PHONESET_DND_METHOD : SEND_BUSY

**Interface:**
- Browser — Administration: Phone Configuration
- File — user-config

**Access:** Admin only

### Time

**PHONESET_TIME_DST_RULE** : <rule>

Schedule for applying daylight saving time.

- **Default:** If null, NORTH_AMERICA is used.
- **Options:** NONE, NORTH_AMERICA, or WESTERN_EUROPE
- **Min/max:** 0/1
- **Example:** PHONESET_TIME_DST_RULE : NORTH_AMERICA

**Interface:**
- Phonetop — Prefs: Time & Locale
- Browser — Preferences: Preferences
- File — user-config

**Access:** All users
**PHONESET_TIME_OFFSET**: <minutes>

Difference in minutes between the phone's local time and Greenwich Mean Time.

**Default:** If null, -300 is used.

**Options:** + or - followed by a numeric multiple of 60; multiples of 30 or 15 also accepted

**Min/max:** 0/1

**Examples:**

PHONESET_TIME_OFFSET : +120
PHONESET_TIME_OFFSET : -480

**Interface:**

Phonetop — Prefs: Time & Locale
Browser — Preferences: Preferences
File — user-config

**Access:** All users

**PHONESET_TIME_SERVER**: <address>

The IP address or host name of a specific time server for an xpressa phone to use.

**Default:** See page 61.

**Options:** Alphanumeric

**Min/max:** 0/1

**Examples:**

PHONESET_TIME_SERVER : 140.79.17.101
PHONESET_TIME_SERVER : clock.isc.org

**Interface:**

Phonetop — Prefs: Network Settings
Browser — Administration: Phone Configuration
File — user-config

**Access:** Admin only
Appendix B: Parameter reference

Network management

**PHONESET_HTTP_PORT**: `<port number>`

The port number for the xpressa phone’s embedded web server. A value greater than 0 enables the web server so that the browser-based interface or MyPingtel user portal can be used with the phone.

**Default**: 80 for xpressa phones
Null (disabled) for instant xpressa softphones

**Options**: Numeric: Two or four digits
A value less than or equal to 0 disables the web server.

**Min/max**: 0/1

**Example**: `PHONESET_HTTP_PORT : 8080`

**Interface**: Phonetop — Prefs: myxpressa Web
Browser — Administration: Phone Configuration
File — user-config

**Access**: Admin only

**PHONESET_MYPINGTEL_PHONE_ID**: `<ID>`

A unique identifier supplied by the MyPingtel user portal to each registered phone.

**Default**: None

**Options**: N/A: Supplied by the MyPingtel sign-in application only.

**Min/max**: 0/1

**Example**: `PHONESET_MYPINGTEL_PHONE_ID : 253`

**Interface**: MyPingtel — MyPingtel sign-in (phonetop)
File — user-config

**Access**: Users set this value when they sign the phone in or out of the MyPingtel user portal with the MyPingtel sign-in xpression.
**PHONESET_MYPINGTEL_SERVER : <URL>**

Stores my.pingtel.com for phones that are registered for the MyPingtel user portal.

- **Default:** None
- **Options:** N/A: Supplied by the MyPingtel sign-in application only.
- **Min/max:** 0/1
- **Example:** PHONESET_MYPINGTEL_SERVER : my.pingtel.com
- **Interface:** MyPingtel — MyPingtel sign-in (phonetop)
  File — user-config
- **Access:** Users set this value when they sign the phone in or out of the MyPingtel user portal with the MyPingtel sign-in xpression.

**PHONESET_MYPINGTEL_USERNAME : <name>**

The user name of a registered MyPingtel user. PHONESET_HTTP_AUTH_DB also stores this user name along with the encrypted password.

- **Default:** None
- **Options:** N/A: Supplied by the MyPingtel sign-in application only.
- **Min/max:** 0/1
- **Example:** PHONESET_MYPINGTEL_USERNAME : jsmith
- **Interface:** MyPingtel — MyPingtel sign-in (phonetop)
  File — user-config
- **Access:** Users set these values when they sign the phone in or out of the MyPingtel user portal with the MyPingtel sign-in xpression.
Appendix B: Parameter reference

**PHONESET_SNMP_TRAP_DESTS : <address> <address> <address>**

The IP address(es) or host name(s) of network management SNMP stations. Enter up to eight on a single line, separated by spaces. Enables SNMP trap messaging.

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:**

  ```
  PHONESET_SNMP_TRAP_DESTS : 10.69.14.2 sip.srvr.com
  ```

- **Interface:** Browser — Administration: Phone Configuration
  File — user-config
- **Access:** Admin only

**PHONESET_MSG_WAITING_SUBSCRIBE : <address>**

The address of a network voice mail server. If an address is present, each time the xpressa phone restarts it sends a SIP SUBSCRIBE message to this server to discover status changes to voice mail.

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:**

  ```
  PHONESET_MSG_WAITING_SUBSCRIBE : sip:usr@vm.hipsrv.com
  ```

- **Interface:** Browser — Administration: Phone Configuration
  File — user-config
- **Access:** Admin only
**PHONESET_VOICEMAIL_RETRIEVE** : <address>

The retrieval address on a network voice mail server. Enables simple retrieval of messages in a target mailbox from an xpressa phone.

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:**
  
  PHONESET_VOICEMAIL_RETRIEVE : sip:usr@vm.hipsrv.com

- **Interface:** Browser — Administration: Phone Configuration
  
  File — user-config

- **Access:** Admin only

**PHONESET_NETWORK_DUPLEX** : <mode>

The Ethernet performance mode for the xpressa phone to use. Does not apply to instant xpressa softphones.

- **Default:** HALF
- **Options:** FULL or HALF
- **Min/max:** 1/1
- **Example:**
  
  PHONESET_NETWORK_DUPLEX : FULL

- **Interface:**
  
  Browser — Administration: Phone Configuration
  
  File — user-config

- **Access:** Admin only
Appendix B: Parameter reference

Home screen display

PHONESET_LOGO_URL : <URL>
The address of an image file on a web server to display on the home screen.
  Default: None
  Options: Alphanumeric
  Min/max: 0/1
  Example:
    PHONESET_LOGO_URL : http://10.1.1.123/logo.jpg
  Interface: Browser — Administration: Phone Configuration
  File — user-config
  Access: Admin only

SIP servers

SIP_DIRECTORY_SERVERS : sip:<host name>
The address of the server that provides location services for call requests.
  Default: None
  Options: Alphanumeric
  Min/max: 0/1
  Example:
    SIP_DIRECTORY_SERVERS : sip:sip.hipsersive.com
  Interface: Browser — Administration: Phone Configuration
  File — pinger-config
  Access: Admin only
**SIP_PROXY_SERVERS** : sip:<host name>

The address of the server that provides firewall or filtering services before forwarding call requests.

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:** SIP_PROXY_SERVERS : sip:sip.hipservice.com
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

**SIP_REGISTER_PERIOD** : <seconds>

The number of seconds before this xpressa phone’s registration with the SIP_REGISTRY_SERVERS expires.

- **Default:** 3600
- **Options:** Numeric
- **Min/max:** 1/1
- **Example:** SIP_REGISTER_PERIOD : 7200
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

**SIP_REGISTRY_SERVERS** : sip:<host name>

The address of the server to which the xpressa phone sends its SIP URL.

- **Default:** None
Appendix B: Parameter reference

**SIP_REGISTRY_SERVERS** : sip:<host name>

- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:** SIP_REGISTRY_SERVERS : sip:sip.hipserservice.com
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

**SIP_ADDRESS** : <address>

If no SIP_REGISTRY_SERVERS is defined, stores a From URL address to send in all SIP messages.

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:** SIP_ADDRESS : sip.pingtel.com
- **Interface:** Browser — Administration: Phone Configuration and use the Additional Parameters section
  File — user-config
- **Access:** Admin only

**SIP messaging**

**SIP_SESSION_REINVITE_TIMER** : <seconds>

A frequency in seconds between the SIP session reinvite messages for this xpressa phone to send during calls. Storing a value enables session reinvite messaging.

- **Default:** Null (disabled)
- **Options:** Numeric
### SIP_SESSION_REINVITE_TIMER

- **Min/max:** 0/1
- **Example:** SIP_SESSION_REINVITE_TIMER : 12
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

### SIP_TCP_PORT

The port on which SIP TCP messages are expected.

- **Default:** 5060
- **Options:** Numeric: Two or four digits
  Should be the same as the value for SIP_UDP_PORT.
- **Min/max:** 1/1
- **Example:** SIP_TCP_PORT : 5062
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

### SIP_UDP_PORT

The port on which SIP UDP messages are expected.

- **Default:** 5060
- **Options:** Numeric: Two or four digits
  Should be the same as the value for SIP_TCP_PORT.
- **Min/max:** 1/1
- **Example:** SIP_UDP_PORT : 5062
Appendix B: Parameter reference

SIP_UDP_PORT: <port number>

- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

**SIP authentication: Incoming calls**

SIP_AUTHENTICATE_DB.<user_name> : <password>

Stores the user ID and password that must be sent to this xpressa phone with an incoming call.

- **Default:** None
- **Options:** Alphanumeric user name and alphanumeric password
- **Min/max:** 0/unlimited
- **Example:** SIP_AUTHENTICATE_DB.friend : opensesame

- **Interface:** Browser — Administration: Phone Configuration
  File — user-config
- **Access:** Admin only

SIP_AUTHENTICATE_REALM : <name>

The name of the realm to which incoming call authentication applies.

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:** SIP_AUTHENTICATE_REALM : ENTERPRISE

- **Interface:** Browser — Administration: Phone Configuration
  File — user-config
**SIP_AUTHENTICATE_SCHEME : <HTTP scheme>**

A standard HTTP scheme for authenticating incoming calls.

- **Default:** None
- **Options:** BASIC or DIGEST
- **Min/max:** 0/1
- **Example:** SIP_AUTHENTICATE_SCHEME : DIGEST
- **Interface:** Browser — Administration: Phone Configuration
  File — user-config
- **Access:** Admin only

**SIP authentication: Outgoing calls**

**SIP_AUTHORIZE_PASSWORD.<realm ID> : <password>**

Stores a destination that requires authentication and the password it requires.

- **Default:** None
- **Options:** Alphanumeric SIP URL or realm identifier and alphanumeric password
- **Min/max:** 0/unlimited
- **Example:** SIP_AUTHORIZE_PASSWORD.sip.hpsrv.net : password
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only
Appendix B: Parameter reference

### SIP_AUTHORIZE_USER.<realm ID> : <user name>

Stores a destination that requires authentication and the user name it requires.

- **Default:** None
- **Options:** Alphanumeric SIP URL or realm identifier and alphanumeric user name
- **Min/max:** 0/unlimited
- **Example:**
  
  ```
  SIP_AUTHORIZE_USER.sip.hipsrv.net : user_name
  ```
- **Interface:**
  - Browser — Administration: Phone Configuration
  - File — pinger-config
- **Access:** Admin only

### Firewalls

#### PHONESET_EXTERNAL_IP_ADDRESS : <IP address>

The IP address for an xpressa phone that is behind a firewall to send in SIP messages. This alerts the other SIP user agent(s) in the call that this is the address to which SIP, RTP, and RTCP packets should be sent.

- **Default:** None
- **Options:** Alphanumeric
- **Min/max:** 0/1
- **Example:**
  
  ```
  PHONESET_EXTERNAL_IP_ADDRESS : 209.251.66.16
  ```
- **Interface:**
  - Browser — Administration: Phone Configuration
  - File — pinger-config
- **Access:** Admin only
**PHONESET_HTTP_PROXY_HOST**: `<host name>`

The proxy host for HTTP transactions. With `PHONESET_HTTP_PROXY_PORT`, allows an xpressa phone that is behind a proxied firewall to download xpression applications from a remote server.

- **Default**: None
- **Options**: Alphanumeric
- **Min/max**: 0/1
- **Example**: `PHONESET_HTTP_PROXY_HOST : proxy.hipsrie.com`
- **Interface**: Browser — Administration: Phone Configuration
  - File — user-config
- **Access**: Admin only

**PHONESET_HTTP_PROXY_PORT**: `<proxy port number>`

The proxy port for HTTP transactions. With `PHONESET_HTTP_PROXY_HOST`, allows an xpressa phone that is behind a proxied firewall to download xpression applications from a remote server.

- **Default**: None
- **Options**: Numeric: Two or four digits
- **Min/max**: 0/1
- **Example**: `PHONESET_HTTP_PROXY_PORT : 8080`
- **Interface**: Browser — Administration: Phone Configuration
  - File — user-config
- **Access**: Admin only
Appendix B: Parameter reference

QoS

`PHONESET_RTP_PORT_START : <port number>`

The port number for audio media received by the xpressa phone in RTP packets. The next consecutively numbered port receives RTCP control packets.

- **Default:** 8766
- **Options:** Numeric: Two or four digits
- **Min/max:** 1/1
- **Example:** `PHONESET_RTP_PORT_START : 8016`
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

pingtel.net calling service

`PHONESET_ADMIN_DOMAIN : <name>`

The name of an xpressa phone’s administrative domain.

- **Default:** None
- **Options:** N/A: Supplied by the pingtel.net service only.
- **Min/max:** 0/1
- **Example:** `PHONESET_ADMIN_DOMAIN : your_domain`
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only
### PHONESET_DEPLOYMENT_SERVER : <address>

The URL for the pingtel.net service.

- **Default:** None
- **Options:** N/A: pds.pingtel.net/deployment only
- **Min/max:** 0/1
- **Example:** N/A
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only; users set this value when they sign in with the pingtel.net service xpression. See page 104.

### PHONESET_LOGICAL_ID : <name>

An identifying key for an xpressa phone using the pingtel.net calling service.

- **Default:** None
- **Options:** N/A: Supplied by the pingtel.net service only.
- **Min/max:** 0/1
- **Example:** PHONESET_LOGICAL_ID : your_username
- **Interface:** Browser — Administration: Phone Configuration
  File — pinger-config
- **Access:** Admin only

### Troubleshooting

### ALLOW_CONSOLE_OUTPUT : <destination>

Directs output to the console.

- **Default:** Null: no output produced
### ALLOW_CONSOLE_OUTPUT : <destination>  
**Options:** ENABLE or null.  
**Min/max:** 0/1  
**Example:** ALLOW_CONSOLE_OUTPUT : ENABLE  
**Interface:** Browser — Administration: Phone Configuration  
File — user-config  
**Access:** Admin only

### JAVA_OUTPUTSTREAM_REDIRECT : <destination>  
Directs Java debugging output to the console.  
**Default:** Null: no output produced  
**Options:** CONSOLE or null.  
**Min/max:** 0/1  
**Example:** JAVA_OUTPUTSTREAM_REDIRECT : CONSOLE  
**Interface:** Browser — Administration: Phone Configuration  
File — user-config  
**Access:** Admin only
## Appendix C: Alphabetical parameter index

For reference, this appendix lists every configuration parameter in alphabetical order. Click on any parameter name or page reference to go directly to its description.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALLOW_CONSOLE_OUTPUT</td>
<td>page 141</td>
</tr>
<tr>
<td>JAVA_OUTPUTSTREAM_REDIRECT</td>
<td>page 142</td>
</tr>
<tr>
<td>PHONESET_ADMIN_DOMAIN</td>
<td>page 106</td>
</tr>
<tr>
<td>PHONESET_AVAILABLE_BEHAVIOR</td>
<td>page 57</td>
</tr>
<tr>
<td>PHONESET_BUSY_BEHAVIOR</td>
<td>page 58</td>
</tr>
<tr>
<td>PHONESET_CALL_WAITING_BEHAVIOR</td>
<td>page 58</td>
</tr>
<tr>
<td>PHONESET_DEPLOYMENT_SERVER</td>
<td>page 106</td>
</tr>
<tr>
<td>PHONESET_DIALPLAN_LENGTH</td>
<td>page 47</td>
</tr>
<tr>
<td>PHONESET_DIGITMAP</td>
<td>page 48</td>
</tr>
<tr>
<td>PHONESET_DND</td>
<td>page 59</td>
</tr>
<tr>
<td>PHONESET_DND_METHOD</td>
<td>page 59</td>
</tr>
<tr>
<td>PHONESET_EXTENSION</td>
<td>page 46</td>
</tr>
<tr>
<td>PHONESET_EXTERNAL_IP_ADDRESS</td>
<td>page 96</td>
</tr>
<tr>
<td>PHONESET_HTTP_AUTH_DB</td>
<td>page 54</td>
</tr>
<tr>
<td>PHONESET_HTTP_PORT</td>
<td>page 64</td>
</tr>
<tr>
<td>PHONESET_HTTP_PROXY_HOST</td>
<td>page 99</td>
</tr>
<tr>
<td>PHONESET_HTTP_PROXY_PORT</td>
<td>page 99</td>
</tr>
<tr>
<td>PHONESET_LOGICAL_ID</td>
<td>page 106</td>
</tr>
</tbody>
</table>
## Appendix C: Alphabetical parameter index

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHONESET_LOGO_URL</td>
<td>page 70</td>
</tr>
<tr>
<td>PHONESET_MSG_WAITING_SUBSCRIBE</td>
<td>page 66</td>
</tr>
<tr>
<td>PHONESET_MYPINGTEL_PHONE_ID</td>
<td>page 64</td>
</tr>
<tr>
<td>PHONESET_MYPINGTEL_SERVER</td>
<td>page 64</td>
</tr>
<tr>
<td>PHONESET_MYPINGTEL_USERNAME</td>
<td>page 65</td>
</tr>
<tr>
<td>PHONESET_NETWORK_DUPLEX</td>
<td>page 69</td>
</tr>
<tr>
<td>PHONESET_NO_ANSWER_TIMEOUT</td>
<td>page 58</td>
</tr>
<tr>
<td>PHONESET_RINGER</td>
<td>page 56</td>
</tr>
<tr>
<td>PHONESET_RTP_PORT_START</td>
<td>page 103</td>
</tr>
<tr>
<td>PHONESET_SNMP_TRAP_DESTS</td>
<td>page 68</td>
</tr>
<tr>
<td>PHONESET_TELNET_ACCESS</td>
<td>page 55</td>
</tr>
<tr>
<td>PHONESET_TIME_DST_RULE</td>
<td>page 62</td>
</tr>
<tr>
<td>PHONESET_TIME_OFFSET</td>
<td>page 62</td>
</tr>
<tr>
<td>PHONESET_TIME_SERVER</td>
<td>page 61</td>
</tr>
<tr>
<td>PHONESET_VOICEMAIL_RETRIEVE</td>
<td>page 66</td>
</tr>
<tr>
<td>SIP_ADDRESS</td>
<td>page 86</td>
</tr>
<tr>
<td>SIP_AUTHENTICATE_DB</td>
<td>page 93</td>
</tr>
<tr>
<td>SIP_AUTHENTICATE_REALM</td>
<td>page 92</td>
</tr>
<tr>
<td>SIP_AUTHENTICATE_SCHEME</td>
<td>page 92</td>
</tr>
<tr>
<td>SIP_AUTHORIZE_PASSWORD</td>
<td>page 91</td>
</tr>
<tr>
<td>SIP_AUTHORIZE_USER</td>
<td>page 89</td>
</tr>
<tr>
<td>Parameter name</td>
<td>See...</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SIP_DIRECTORY_SERVERS</td>
<td>page 85</td>
</tr>
<tr>
<td>SIP_FORWARD_ON_BUSY</td>
<td>page 59</td>
</tr>
<tr>
<td>SIP_FORWARD_ON_NO_ANSWER</td>
<td>page 57</td>
</tr>
<tr>
<td>SIP_FORWARD_UNCONDITIONAL</td>
<td>page 57</td>
</tr>
<tr>
<td>SIP_PROXY_SERVERS</td>
<td>page 87</td>
</tr>
<tr>
<td>SIP_REGISTER_PERIOD</td>
<td>page 86</td>
</tr>
<tr>
<td>SIP_REGISTRY_SERVERS</td>
<td>page 86</td>
</tr>
<tr>
<td>SIP_SESSION_REINVITE_TIMER</td>
<td>page 88</td>
</tr>
<tr>
<td>SIP_TCP_PORT</td>
<td>page 88</td>
</tr>
<tr>
<td>SIP_UDP_PORT</td>
<td>page 88</td>
</tr>
</tbody>
</table>
Index

802.1p 102
911, digitmap for 50

A
About screen
IP address and 5
network settings and 22
software versions and 109
ACK method, SIP 149
addressing SIP calls 78
admin password 38
administrative security
changing the password 41
logging on 39
resetting the password 43, 115
using 38
alerts for incoming calls 56
app-config file 111
audio files, replacing 117
authentication
incoming calls 92
outgoing calls 89
parameters for 88
automating dialing 47

B
bit markings, TOS 101
browser-based interface 3
controlling access 63
instant xpressa and 64
logging on to 40
user access 44
using 26
BYE method, SIP 149

C
call control methods 149
call handling parameters 55
call forwarding 57
call waiting 58
do not disturb 59
CANCEL method, SIP 149
changing
configuration parameters 24
installed applications 111
network settings 18
passwords 41, 44
configuration files
app-config 111
default values 35
editing 29
format used in 29
pinger-config 28
reviewing 34
user-config 28
configuration parameters
authentication 88, 178
browser access 54
call handling 55, 163
dialing 46, 160
files for 28
firewall access 95, 180
interfaces for changing 24
network management 63, 170
phone security 54, 162
pingtel.net calling service 106, 182
QoS 182
setting 24
SIP messaging 88, 176
SIP server 85, 174
time 61, 168
troubleshooting 183
configuring xpressa phones 24

D

daylight saving time 62
default configuration 35
defaults, reverting to 115
defining
  external IP address 96
  SIP Directory server 85
  SIP Proxy server 87
  SIP Registry server 86
  DHCP network settings 18
dialing 911 50
dialing parameters 46
dialplan length 47
DiffServ 101
digit maps 48
Directory servers, SIP
  background 73
  parameter for 85
  SIP Location servers and xpressa phones and 73
disabling web access 63
DNS server(s), setting static 19
Do Not Disturb feature 59
Domain Name System (DNS) server 19
Dynamic Host Configuration Protocol (DHCP) 18

E

embedded web server 3, 64
enabling
  session timer 88
  web access 63
error codes, JTAPI 124
extensions, setting 46
external IP address, setting 96
factory defaults 115
firewalls 94
configuring 94
external IP address for 96
NAT 97
proxyed 99
gateway, setting static 20
getting started
call testing 5
calling service calls 8
evaluation 5
installation 12
network configuration 18
objectives 4
setting extensions 46
SIP environments 7
graphics, home screen 59, 70
N
NAT firewalls 97
net mask, setting static 20
Network Address Translation (NAT) 97
network management parameters 63
network settings 18
    DHCP 18
    static 20
    verifying 22
new releases, installing 107
NOTIFY method, SIP 149

O
operating system 2
    upgrading 107
    version, finding 109
OPTIONS method, SIP 149
outgoing call authentication 88

P
parameters, configuration 24, 160, 185
passwords
    admin 38
    user 44
peer-to-peer calling 5
phone logs 128
phonetop interface 3, 25
logging on to 40
PIM, installing phones with 12
pinger-config
    configuration file 28
    default values 35
Pingtel Deployment Server (PDS) 9
pingtel.net calling service
    configuration parameters 106
    registering a phone 104
    starting 105
    stopping 105
    user name and password 104
    port mapping, SIP and RTP 95, 97
ports
    firewalls and 94
    HTTP proxy 99
    HTTP server 64
    RTP and RTCP 96
    SIP TCP and UDP 96
Power Insertion Module (PIM) 12
powering options 13
Prefs xpression 25
proxied firewalls 99
Proxy servers, SIP
    as Directory server 74
    background 77
    definition 157
    parameter for 87
    xpressa phones and 77
    proxy settings, HTTP 99
Quality of Service (QoS) 101
R
Real-time Control Protocol (RTCP) 103
Real-time Transport Protocol (RTP) 103
Redirect servers, SIP 77
    as Directory server 75
    definition 157
## Index

<table>
<thead>
<tr>
<th>REFERENCE</th>
<th>PAGE</th>
<th>REFERENCE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>REFER method, SIP</td>
<td>149</td>
<td>static network values</td>
<td>20</td>
</tr>
<tr>
<td>REGISTER method, SIP</td>
<td>149</td>
<td>time display</td>
<td>61</td>
</tr>
<tr>
<td>Registry servers, SIP</td>
<td></td>
<td>setting up users</td>
<td>44</td>
</tr>
<tr>
<td>background</td>
<td>72</td>
<td>signing in to pingtel.net</td>
<td>105</td>
</tr>
<tr>
<td>definition</td>
<td>157</td>
<td>Simple Network Management Protocol (SNMP)</td>
<td>67</td>
</tr>
<tr>
<td>parameters for xpressa phones and releases, installing</td>
<td>86</td>
<td>Simple Network Time Protocol (SNTP)</td>
<td>61</td>
</tr>
<tr>
<td>replacing software files</td>
<td>72</td>
<td>SIP</td>
<td></td>
</tr>
<tr>
<td>response codes, SIP</td>
<td>107</td>
<td>addresses</td>
<td>155</td>
</tr>
<tr>
<td>restarting an xpressa phone</td>
<td>113</td>
<td>environments</td>
<td>71</td>
</tr>
<tr>
<td>reverting to factory defaults</td>
<td>115</td>
<td>features, supported</td>
<td>158</td>
</tr>
<tr>
<td>reviewing configuration files</td>
<td>112</td>
<td>messages</td>
<td>148</td>
</tr>
<tr>
<td>ring tone, replacing</td>
<td>117</td>
<td>parameters</td>
<td>85</td>
</tr>
<tr>
<td>RTCP ports</td>
<td>103</td>
<td>phone environments</td>
<td>71</td>
</tr>
<tr>
<td>RTP ports</td>
<td>103</td>
<td>servers</td>
<td>71, 85</td>
</tr>
<tr>
<td>S</td>
<td></td>
<td>SIP calls</td>
<td>156</td>
</tr>
<tr>
<td>security</td>
<td></td>
<td>SIP sessions</td>
<td>156</td>
</tr>
<tr>
<td>administrative log on</td>
<td>38</td>
<td>SIP transactions</td>
<td>155</td>
</tr>
<tr>
<td>browser-based interface</td>
<td>38</td>
<td>user agents</td>
<td>157</td>
</tr>
<tr>
<td>configuration parameters</td>
<td>40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>phonetop interface</td>
<td>40</td>
<td>SNMP messages</td>
<td>67</td>
</tr>
<tr>
<td>protected tasks</td>
<td>38</td>
<td>software upgrades, installing</td>
<td>107</td>
</tr>
<tr>
<td>selecting incoming call alerts</td>
<td>56</td>
<td>software version</td>
<td></td>
</tr>
<tr>
<td>serial number</td>
<td>11, 127, 145</td>
<td>determining</td>
<td>109</td>
</tr>
<tr>
<td>session reinvite messaging</td>
<td>88</td>
<td>finding</td>
<td>109</td>
</tr>
<tr>
<td>setting</td>
<td></td>
<td>startup audio, replacing</td>
<td>117</td>
</tr>
<tr>
<td>configuration values</td>
<td>24</td>
<td>startup, xpressa phone</td>
<td>16</td>
</tr>
<tr>
<td>daylight saving time</td>
<td>62</td>
<td>static network settings</td>
<td>20</td>
</tr>
<tr>
<td>extensions</td>
<td>46</td>
<td>support services, Pingtel</td>
<td>10</td>
</tr>
<tr>
<td>SIP registration</td>
<td>86</td>
<td>system components, SIP</td>
<td>156</td>
</tr>
</tbody>
</table>

---

**Note:** The above index contains terms and references typically found in a document related to telecommunication settings and configurations. This includes methods of communication, server setups, and various system parameters and features. The page numbers indicate where these terms are discussed in the document. The index captures the essence of the document’s content, providing a navigational aid for readers to quickly locate specific sections or concepts.
| T | Technical Assistance Center (TAC) 11, 38, 145 |
|   | Telnet access 55 |
|   | time parameters 61 |
|   | time server, specifying 61 |
|   | time zone 62 |
|   | trap messages, SNMP 67 |
|   | troubleshooting 119 |
|   | configuration parameters 141 |
|   | configuration review 144 |
|   | using logs 128 |
|   | type of service (TOS) 101 |

| U | upgrade log 142 |
|   | upgrading software 107 |
|   | User Agent Client (UAC) 157 |
|   | User Agent Server (UAS) 157 |
|   | user interface 3 |
|   | browser-based 3 |
|   | phonetop 3 |
|   | user-config 28 |
|   | configuration file 28 |
|   | default values 35 |
|   | users, browser access for using 44 |
|   | basic services 6 |

| V | VersionCheck 108 |
|   | versions, finding 109 |
|   | virtual LAN (VLAN) 102 |
|   | voice mail 7 |
|   | call forwarding to 57 |
|   | message waiting indication 65 |
|   | retrieving 66 |
|   | subscribing 66 |
|   | VxWorks 2 |
|   | web access, controlling 63 |
|   | web server, phone 3, 64 |
|   | web site, Pingtel 10 |

| W | xpressa Development Kit (xDK) 3, 9 |
|   | xpressa home screen 17, 114 |
|   | xpressa phone 46 |
|   | configuring 24 |
|   | factory defaults 115 |
|   | installing 12 |
|   | introduction 1 |
|   | powering options 13 |
|   | restarting 113 |
|   | xpressa splash screen 17, 113 |
|   | xpression applications 2 |
|   | managing 111 |
|   | Prefs 25 |
Installing & Configuring Pingtel phones
Pingtel xpressa™
Pingtel instant xpressa™
Release 1.2
P/N 039-011-002