



Aastra BluStar[™] 8000i Desktop Media Phone



SIP Call Server Administrator Guide

Release 4.1.1

Software License Agreement

Aastra Telecom Inc., hereinafter known as "Seller", grants to Customer a personal, worldwide, non-transferable, non-sub-leaseable and non-exclusive, restricted use license to use Software in object form solely with the Equipment for which the Software was intended. This Product may integrate programs, licensed to Aastra by third party Suppliers, for distribution under the terms of this agreement. These programs are confidential and proprietary, and are protected as such by copyright law as unpublished works and by international treaties to the fullest extent under the applicable law of the jurisdiction of the Customer. In addition, these confidential and proprietary programs are works conforming to the requirements of Section 401 of title 17 of the United States Code. Customer shall not disclose to any third party such confidential and proprietary programs and information and shall not export licensed Software to any country except in accordance with United States Export laws and restrictions.

Customer agrees to not reverse engineer, decompile, disassemble or display Software furnished in object code form. Customer shall not modify, copy, reproduce, distribute, transcribe, translate or reduce to electronic medium or machine readable form or language, derive source code without the express written consent of the Seller and its Suppliers, or disseminate or otherwise disclose the Software to third parties. All Software furnished hereunder (whether or not part of firmware), including all copies thereof, are and shall remain the property of Seller and its Suppliers and are subject to the terms and conditions of this agreement. All rights reserved.

Customer's use of this software shall be deemed to reflect Customer's agreement to abide by the terms and conditions contained herein. Removal or modification of trademarks, copyright notices, logos, etc., or the use of Software on any Equipment other than that for which it is intended, or any other material breach of this Agreement, shall automatically terminate this license. If this Agreement is terminated for breach, Customer shall immediately discontinue use and destroy or return to Seller all licensed software and other confidential or proprietary information of Seller. In no event shall Seller or its suppliers or licensors be liable for any damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of business information, other pecuniary loss, or consequential damages) arising out of the use of or inability to use the software, even if Seller has been advised of the possibility of such damages.

Content

Software License Agreement	ii
Welcome	Preface-i
<i>About this Guide</i>	Preface-i
<i>Audience</i>	Preface-i
<i>Documentation</i>	Preface-i
<i>Upgrading BluStar 8000i Software</i>	Preface-i
<i>Safety Summary</i>	Preface-ii
<i>Obtaining Assistance</i>	Preface-ii
Chapter 1:	
System Overview	1-1
BluStar 8000i Hardware Features	1-2
<i>Screen & LCD Camera</i>	1-2
<i>Phone Features & Keys</i>	1-3
<i>Key Descriptions</i>	1-4
Telephone Feature Controls	1-5
Audio/Video Controls	1-8
App & Telephone Connection Management Controls	1-9
Getting Started	1-10
<i>Plugging In and Starting the BluStar 8000i</i>	1-10
<i>Logging In</i>	1-10
<i>Login Screens</i>	1-11
<i>Fingerprint Reader</i>	1-12
<i>Logging Off / Restarting</i>	1-14
Touch Screen Basics	1-15
<i>On-Screen Keyboard</i>	1-15
<i>Home Screen</i>	1-17
<i>Call Screen</i>	1-23
<i>Lock Screen</i>	1-23

SIP Call Server Installation Information	1-25
<i>Description</i>	1-25
<i>Installation Considerations</i>	1-25
<i>Installation Requirements</i>	1-25
<i>Configuration Server Requirements</i>	1-26
Chapter 2:	
Configuration Server & Files	2-1
Configuration Files	2-1
<i>Update URL</i>	2-2
<i>Configuration Precedence</i>	2-2
<i>Installing the Configuration Files</i>	2-3
<i>Using the Configuration Files</i>	2-3
<i>Encryption</i>	2-4
Configuration Server	2-10
<i>Configuration Server Protocol</i>	2-10
<i>Configuration Server Settings</i>	2-10
<i>Configuring the Configuration Server Protocol</i>	2-13
<i>Configuration Server Redundancy via DNS A Records</i>	2-13
<i>Using the Auto-Resync Feature</i>	2-13
Chapter 3:	
Configuring Network Features	3-1
Network Settings	3-1
<i>Basic Network Settings</i>	3-1
<i>DHCP</i>	3-3
<i>Configuration Server Download Precedence</i>	3-6
<i>DNS Caching</i>	3-6
<i>Configuring Network Settings Manually</i>	3-6
<i>Configuring LAN and PC Port Negotiation</i>	3-7
<i>Network Time Servers</i>	3-8
<i>Type of Service (ToS), Quality of Service (QoS), and DiffServ QoS</i>	3-8
<i>Virtual Local Area Network (VLAN)</i>	3-9
<i>Virtual Private Network (VPN)</i>	3-10

SIP Account Settings	3-11
<i>Description</i>	3-11
<i>Basic SIP Settings</i>	3-11
<i>Advanced SIP Settings (optional)</i>	3-13
<i>Real-time Transport Protocol (RTP) Settings</i>	3-14

Chapter 4: Configuring Operational Features

BluStar 8000i Settings	4-2
<i>Terminal Identity</i>	4-2
<i>Factory Defaults</i>	4-4
<i>Power Saving Schedule</i>	4-4
<i>User Settings</i>	4-8
<i>Terminal Security Settings</i>	4-8
<i>Screen Settings</i>	4-10
<i>Locale Settings</i>	4-10
<i>Audio/Video Settings</i>	4-11
<i>Call Forward Settings</i>	4-12
<i>Incoming Intercom Call Auto-Answer Settings</i>	4-13
<i>History</i>	4-13
<i>Directory</i>	4-16
<i>Basic LDAP Settings</i>	4-24
<i>Advanced LDAP Settings (optional)</i>	4-27
<i>Microsoft Exchange Contacts</i>	4-30
<i>LDAP Directory/Exchange Contacts Update Interval</i>	4-32
<i>Voicemail</i>	4-33
<i>Video Voicemail Client Integration</i>	4-34
<i>Emergency Dial Plan</i>	4-35
<i>Picture ID Feature</i>	4-36
<i>Busy Lamp Field (BLF)</i>	4-37
<i>BLF Subscription Period</i>	4-38
<i>Directed Call Pickup</i>	4-38
<i>Diversion Display</i>	4-40
<i>Shared Call Appearance (SCA) and SCA Call Bridging</i>	4-41

<i>XML Settings</i>	4-42
<i>Licensing</i>	4-43

Chapter 5: Advanced Operational Features..... 5-1

Advanced Operational Features	5-1
<i>Update Caller ID During a Call</i>	5-1
<i>MAC Address in REGISTER Messages</i>	5-2
<i>SIP Message Sequence for Blind Transfer</i>	5-2
<i>Removing UserAgent and Server SIP Headers</i>	5-2
<i>Removing Inactive Video Streams in the SDP</i>	5-3
<i>Blacklist Duration</i>	5-3
<i>Whitelist Proxy</i>	5-3
<i>XML SIP Notify Events</i>	5-4
<i>Configurable DNS Queries</i>	5-5
<i>Ignore Out of Sequence Errors</i>	5-6
<i>Switching Between Early Media and Local Ringing</i>	5-7
<i>Configurable “Allow” and “Allow-Event” Optional Headers</i>	5-7
<i>Configurable SIP P-Asserted Identity (PAI)</i>	5-7
<i>Configurable Compact SIP Header</i>	5-8
<i>Configurable Dial Plan Terminator</i>	5-9

Chapter 6: Troubleshooting..... 6-1

BluStar 8000i Status	6-1
<i>About</i>	6-1
<i>Status</i>	6-1
<i>Graphic Status Page</i>	6-3
<i>On-Screen Connection Quality Alarms</i>	6-6
Syslog Settings	6-7
<i>Syslog Location</i>	6-7
<i>System-Wide Logging</i>	6-7
<i>SIP Stack Logging</i>	6-8
<i>Debug Logging</i>	6-8

Troubleshooting Solutions	6-9
<i>How do I restart the BluStar?</i>	6-9
<i>How do I set the BluStar to factory default?</i>	6-9
<i>How can I send comments or report a bug concerning my BluStar?</i>	6-10

Appendix A:

Parameters	A-1
Introduction	A-1
<i>Topics</i>	A-1
Setting Parameters in Configuration Files	A-3
Operational, Basic Parameters	A-4
<i>Network Settings</i>	A-4
<i>ToS/QoS/Diffserv QoS Parameters</i>	A-8
<i>Virtual Local Area Network (VLAN) Settings</i>	A-8
<i>DHCP Option Settings</i>	A-10
<i>Configuration Server Settings</i>	A-11
<i>Rport Setting</i>	A-20
<i>SIP Settings</i>	A-20
<i>Advanced SIP Settings</i>	A-25
<i>Directory Settings</i>	A-28
<i>Call History Settings</i>	A-30
<i>Missed Calls Indicator Settings</i>	A-30
<i>Basic LDAP Settings</i>	A-30
<i>Advanced LDAP Settings</i>	A-32
<i>Microsoft Exchange Contact Settings</i>	A-44
<i>LDAP Directory/Exchange Contacts Update Interval</i>	A-47
<i>User Settings</i>	A-49
<i>Power Saving Schedule Settings</i>	A-49
<i>Terminal Security Settings</i>	A-56
<i>Screen Settings</i>	A-58
<i>Locale Settings</i>	A-60
<i>Audio/Video Settings</i>	A-63
<i>Call Forward Settings</i>	A-65
<i>Incoming Intercom Call Auto-Answer Settings</i>	A-68

<i>Voicemail Settings</i>	A-68
<i>Video Voicemail Client Integration Settings</i>	A-69
<i>Emergency Dial Plan Settings</i>	A-70
<i>Picture ID Feature</i>	A-75
<i>BLF List URI Settings</i>	A-75
<i>BLF Subscription Period Settings</i>	A-76
<i>Directed Call Pickup</i>	A-76
<i>XML Settings</i>	A-77
Advanced Operational Parameters	A-78
<i>Update Caller ID Setting</i>	A-78
<i>Blind Transfer Setting</i>	A-78
<i>User-Agent Settings</i>	A-78
<i>Inactive Video Stream Settings</i>	A-79
<i>Blacklist Duration Setting</i>	A-79
<i>Whitelist Proxy Setting</i>	A-79
<i>XML SIP Notify Settings</i>	A-80
<i>DNS Query Setting</i>	A-81
<i>Ignore Out of Order SIP Requests</i>	A-82
<i>Optional “Allow” and “Allow-Event” Headers</i>	A-82
<i>P-Asserted Identity (PAI)</i>	A-82
<i>Compact SIP Header</i>	A-83
<i>Dial Plan Terminator</i>	A-83
Troubleshooting Parameters	A-84
<i>On-Screen Connection Quality Alarms</i>	A-84
<i>Syslog Settings</i>	A-85
<i>Feedback Application Settings</i>	A-90
Appendix B:	
Sample Configuration Files	B-1
<i>Aastra.cfg</i>	B-1
<i><model>.cfg</i>	B-1
<i><Mac>.cfg</i>	B-1
<i><user>.cfg</i>	B-1

Appendix C:	
OpenVPN Configuration	C-1
<i>Server Requirements</i>	C-1
<i>Physical Server and Network Environment</i>	C-1
<i>Configuration Files/Scripts and Certificates/Keys</i>	C-2
<i>Creating the Server-Side Sample Configuration Files/Scripts</i>	C-3
<i>Installing the OpenVPN Server and Creating Certificates/Keys</i>	C-6
<i>Creating the Client-Side Sample Configuration Files/Scripts</i>	C-7
<i>Preparing the Ethernet Bridge and Firewall Rules</i>	C-10
<i>Starting the OpenVPN Service</i>	C-11
<i>Preparing the Configuration Tarball for Remote Terminals</i>	C-11
<i>Configuring the BluStar 8000i Terminal to Enable VPN</i>	C-12
Limited Warranty	Warranty-1
<i>Exclusions</i>	Warranty-1
<i>Warranty Repair Services</i>	Warranty-1
<i>After Warranty Service</i>	Warranty-1
Limited Warranty (Australia Only)	Warranty-2
<i>Repair Notice</i>	Warranty-2
<i>Exclusions</i>	Warranty-2
<i>Warranty Repair Services</i>	Warranty-3
<i>After Warranty Service</i>	Warranty-3
Index	Index-1

Welcome

The Aastra BluStar™ 8000i Desktop Media Phone is designed to enhance the way you communicate and collaborate. Offering true HD video conferencing, the BluStar 8000i uses the latest in video and communications technology to enable a natural high-quality video experience. With its advanced business collaboration features and applications, the BluStar 8000i is a productivity enhancing desktop media phone that is intelligent, intuitive, and easy to use.

About this Guide

This guide explains how to the BluStar 8000i in SIP Call Server mode, which offers generic Session Initiation Protocol (SIP) video phone functionality. This guide also provides information on the basic network setup, operation, and configuration of the BluStar 8000i.

Note:

This guide will be updated periodically with new and/or updated information. For details on what features have been added or updated, please refer to the **Aastra BluStar™ 8000i Desktop Media Phone SIP Call Server Release Notes**.

Audience

This guide is for network administrators, system administrators, developers, and partners who need to understand how to operate and maintain the BluStar 8000i on an open-standards SIP based VoIP deployment. It also provides some user-specific information.

This guide contains information that is at a technical level, more suitable for system or network administrators. A basic knowledge of SIP concepts and the Linux operating system is assumed.

Documentation

The BluStar 8000i documentation consists of the following:

- **Aastra BluStar™ 8000i Desktop Media Phone Quick Start Guide** - Contains installation and set-up instructions, general features and functions, and an overview of the terminal. The English, French, and Simplified Chinese version is included in the box with the BluStar 8000i terminal. The quick start guide is also available in other languages and can be downloaded from <http://www.aastra.com/document-library.htm>.
- **Aastra BluStar™ 8000i Desktop Media Phone SIP Call Server User Guide** - Describes the most commonly used features and functions for an end user when utilizing the BluStar 8000i in SIP Call Server mode.
- **Aastra BluStar™ 8000i Desktop Media Phone BAS-Mode User Guide** - Describes the most commonly used features and functions for an end user when utilizing the BluStar 8000i in BAS mode.
- **Aastra BluStar™ 8000i Desktop Media Phone SIP Call Server Administrator Guide** - Provides all of the configuration options available to configure and deploy the product in SIP Call Server mode.
- **Aastra BluStar™ 8000i Desktop Media Phone BAS-Mode Administrator Guide** - Provides all of the information on how to configure and deploy the product in BAS mode.
- **Aastra BluStar™ 8000i Desktop Media Phone SIP Call Server Release Notes** - Provides new features and documents issues resolved for the BluStar 8000i in SIP Call Server mode.
- **Aastra BluStar™ 8000i Desktop Media Phone BAS-Mode Release Notes** - Provides new features and documents issues resolved for the BluStar 8000i in BAS mode.

Upgrading BluStar 8000i Software

- Procedures for upgrading the BluStar 8000i software are provided in the release notes.

Safety Summary

Please read the following safety information before attempting to install or use the BluStar 8000i.

**Alert!**

For use with included AC/DC adaptor model no. 3A-603DB12 / Pour utiliser avec modèle 3A-603DB12.

**Alert!**

This product is designed for indoor use only and for ambient temperatures at or below 40° C (104° F).

**Warning!**

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

**Warning!**

This product meets the applicable Industry Canada technical specifications.

**Warning!**

Hazardous voltage enclosed. Voltage or current hazard sufficient to cause shock. Disconnect power before servicing.

**Danger!**

There are no operator serviceable parts inside the chassis. Attempting to tamper with the parts inside the chassis may result in serious injury to the user or damage to the equipment.

**Danger!**

This product is designed to work with a single-phase power system having a grounded neutral conductor. To reduce risk of electrical shock, do not plug into any other type of power system.

**Danger!**

The power cord for the terminal functions as the power disconnect device. Ensure that the power cord is readily accessible in case of emergency and for servicing. Disconnect power before servicing.

**Danger!**

Use only the power cord provided. The terminal must use the grounded three-conductor power cord. Do not use two-conductor extension cords.

Obtaining Assistance

If you have read this administrator guide and still have problems, please contact Aastra Telecom Support via one of these methods:

North America

- Toll Free 1-800-574-1611
- Direct +1-469-365-3639
- Online at <http://www.aastratelecom.com/support>, click on Contact Technical Support

Outside North America

Please contact your regional Aastra Technical Support.

Chapter 1

System Overview

This chapter briefly describes the BluStar 8000i and provides information about installing the terminal in SIP Call Server mode.

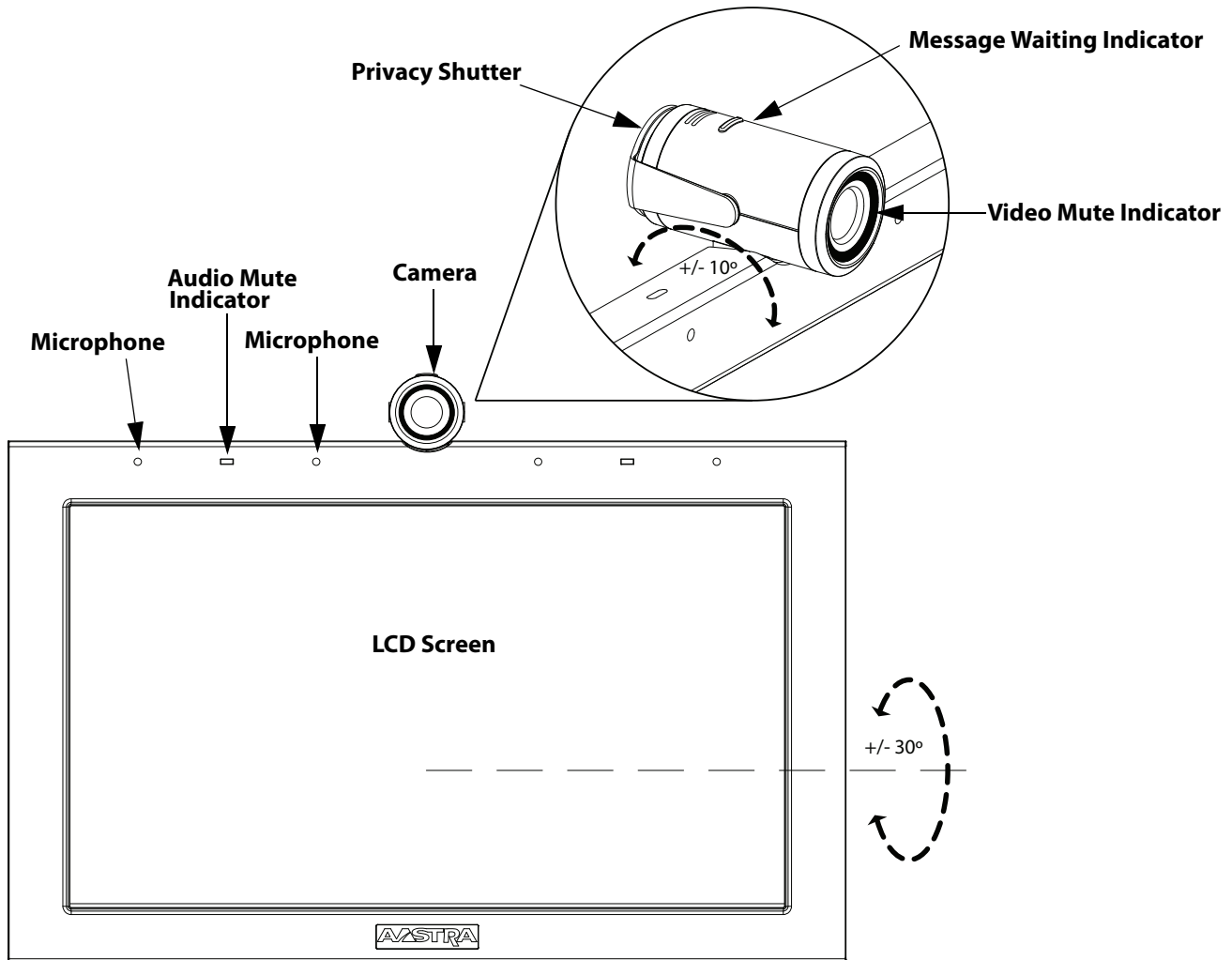
The following information is provided in this chapter:

- [BluStar 8000i Hardware Features](#)
 - [Screen & LCD Camera](#)
 - [Phone Features & Keys](#)
 - [Key Descriptions](#)
- [Telephone Feature Controls](#)
- [Audio/Video Controls](#)
- [App & Telephone Connection Management Controls](#)
- [Getting Started](#)
 - [Plugging In and Starting the BluStar 8000i](#)
 - [Logging In](#)
 - [Login Screens](#)
 - [Fingerprint Reader](#)
 - [Logging Off / Restarting](#)
- [Touch Screen Basics](#)
 - [On-Screen Keyboard](#)
 - [Home Screen](#)
 - [Call Screen](#)
 - [Lock Screen](#)
- [SIP Call Server Installation Information](#)
 - [Description](#)
 - [Installation Considerations](#)
 - [Installation Requirements](#)
 - [Configuration Server Requirements](#)

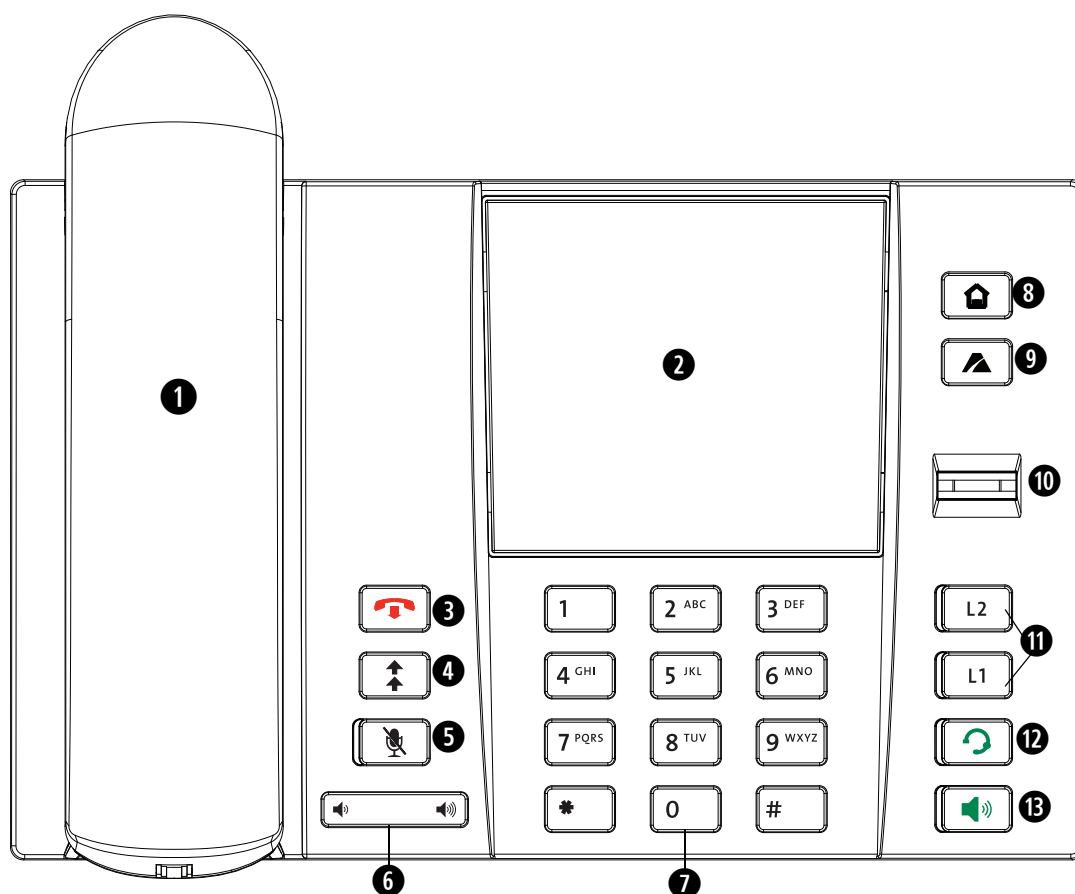
BluStar 8000i Hardware Features

The following two images describe all of the hardware features of the BluStar 8000i:

Screen & LCD Camera














Phone Features & Keys



1	Handset	8	Home Key
2	Speaker	9	Hot Key
3	Goodbye Key	10	Fingerprint Reader
4	Redial Key	11	Line/Call Appearance Key
5	Audio Mute Key	12	Headset Key
6	Volume Key	13	Handsfree Key
7	Keypad		

Key Descriptions

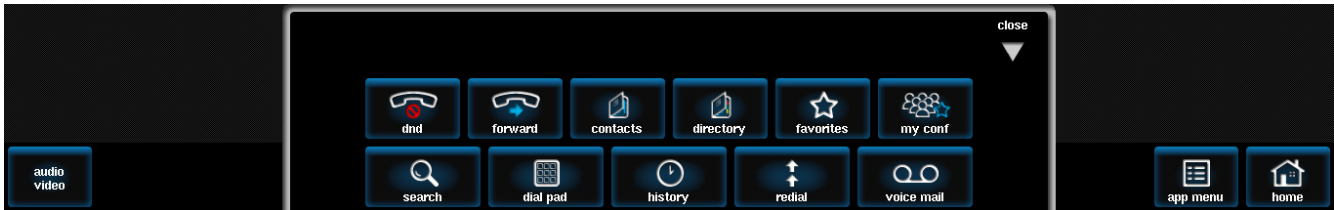
The following table identifies the phone keys on the BluStar 8000i key panel that you can use for handling calls. Users have the options to select different options by pressing the phone keys or by pressing the buttons on the screen. For example, users can increase or decrease the volume level by pressing the **volume control key** OR by pressing the **volume button** in the audio/video controls menu on the screen (see [Telephone Feature Controls](#) on [page 1-5](#)).

Key	Key Description
	Goodbye Key - Ends an active call or conference. The Goodbye key also exits an open list, such as the options list.
	Redial Key - Redials previously dialed numbers. Click on the arrow to access the last 10 dialed numbers.
	Audio Mute Key - Mutes the microphone so that other parties cannot hear you. When your BluStar 8000i is on mute, the audio mute indicator turns red, the LCD beside the audio mute key turns red, and the mute button on the screen is outlined in red.
	Home Key - Opens the home screen.
	Hot Key - Opens or closes the app menu.
	Fingerprint Reader - Users can swipe their finger over the fingerprint reader to login to the BluStar 8000i terminal.
	Line/Call Appearance Keys - Connects you to a line or call. The BluStar 8000i supports 2 line call appearance keys.
	Headset Key - Activates handsfree for making and receiving calls using the headset.
	Handsfree Key - Activates handsfree for making and receiving calls without lifting the handset.
	Volume Control Key - Allows you to adjust the ringer volume on your BluStar 8000i. You can decrease the volume by pressing on the (-) sign and increasing it by pressing the (+) sign. Users can also change the volume by pressing the ring volume button in the audio video controls menu on the screen.
	Keypad Keys - Contains digits 0 - 9, a "*" key, and a "#" key.

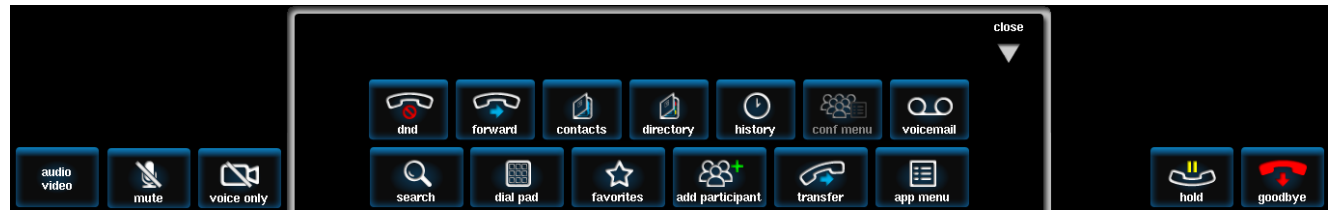
Telephone Feature Controls

The BluStar 8000i has the following telephone feature controls that appear on the Home (or Idle), Call, Conference, and Hold screens. The following images show what applications and controls are available on each screen. You will also notice that different [Audio/Video Controls](#) and [App & Telephone Connection Management Controls](#) are available on each screen.

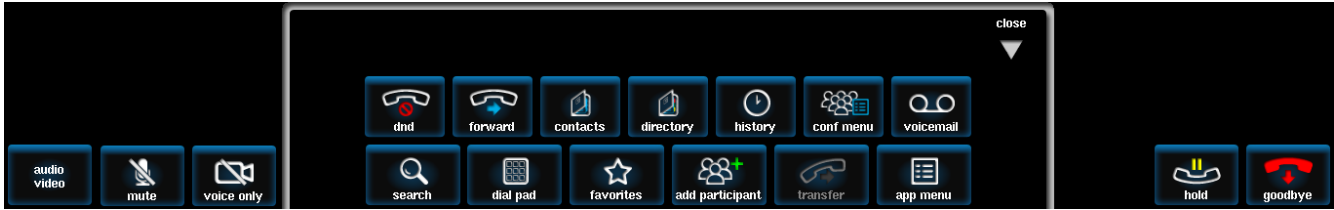
Home/Idle Screen



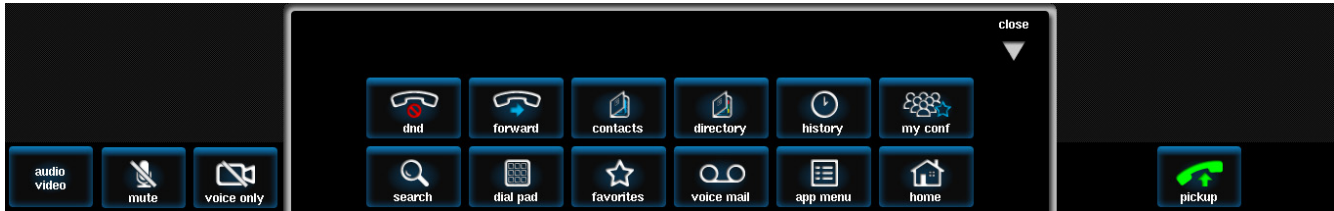
Two-Way Call Screen



Conference Call Screen

















Hold Screen



The following table explains each of the telephone feature controls.

Telephone Feature Controls

Telephone Feature	Description
	Allows you to place the phone in a "Do Not Disturb" (DND) status. If DND is ON, callers calling the phone do not hear a ring and then the call is dropped. If call forward is configured on the phone, the call can be forwarded to voicemail or to another SIP URL or number.
	Allows you to turn ON or OFF call forwarding.
	Stores all of your contact information. On the contacts screen, you can add, edit, and delete contacts. You can also add contacts to your favorites and create contact folders.
	Allows you to find contacts from the global directory.
	Brings up the Favorites menu (the home screen) that displays your favorite contacts.
	Allows you to access your saved conferences. Note: Not available in SIP Call Server mode.
	Allows you to add participants to a conference call.
	Opens the conference menu, where you can request moderator control, change the format, view participants, and save the conference. Note: Not available in SIP Call Server mode.
	Allows you to search through your contacts, favorites, directory, and call history.
	Allows you to dial a SIP URL or phone number.
	Displays information about each call that came to your phone. The BluStar 8000i logs the name and number of the caller, and the date and time of the call.





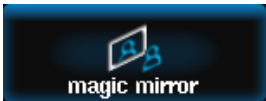



Telephone Feature	Description
	Allows you to redial a phone number. The redial lists stores up to 10 numbers.
	Allows you to access your voicemail to retrieve and listen to stored messages or start the video voicemail client (if configured).
	Allows you to transfer a call to another number, or to connect two active calls together and remove the calls from your BluStar 8000i screen.

Audio/Video Controls

Users can adjust the audio and video settings through the Audio/Video button








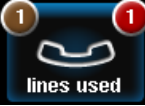



on the main screen. The BluStar 8000i has the following Audio/video controls:

Audio/Video Control	Description
	<p>Allows you to adjust the ringer volume on your BluStar 8000i. You can decrease the volume by pressing the (-) sign and increasing it by pressing the (+) sign. Users can also change the volume by pressing the volume control key on the phone.</p> <p>Note: If you want to adjust the volume of the other party, use the volume button in the call options panel menu on the Call screen.</p>
	<p>Allows you to adjust the tone equalization of the audio heard from the BluStar 8000i speaker while using the speakerphone. You can change the tone equalization to your liking by pressing the (-) and (+) signs.</p>
	<p>Allows you to activate the speakerphone.</p>
	<p>Allows you to activate the headset.</p>
	<p>Opens the magic mirror.</p>
	<p>Turns on self view. When you are in a call or on the Magic Mirror screen, you will be able to see yourself in the bottom right-hand corner of the screen.</p>
	<p>Mutes the microphones on your BluStar 8000i so that other parties cannot hear you.</p> <p>Note: If you want to mute the other party, use the Mute button in the Options menu on the Call screen.</p>
	<p>Turns off the camera so that only voice is available during the call. When you select voice only, you will see the video mute indicator around the camera turn off indicating that the video is turned off. When you de-select it (video is on) the video mute indicator is green.</p>

App & Telephone Connection Management Controls

Users can use the following app and telephone connection management controls while using the BluStar 8000i.

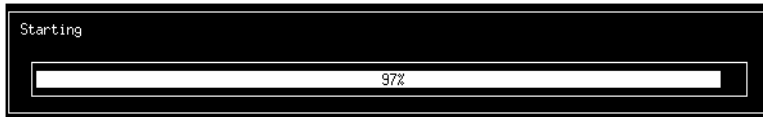
App & Telephone Connection Management Controls	Description
	Opens or closes the App menu.
	Opens the Home screen.
	Allows you to place an active call on hold.
	Allows you to end an active call.
	Allows you to pickup a call that is on hold.
	Allows you to join two or more calls, creating a conference call.
	Shows you how many callers you have placed on hold.
	Shows you how many lines are in use (top-left corner) and how many callers you have placed on hold (top-right corner). Note: Replaces the calls on hold icon when BluStar 8000i terminals are configured for Shared Call Appearance (SCA).
	Allows you to swap between two calls. If Call 1 is on hold and you are speaking with Call 2, you can press the swap button beside Call 1 and it will automatically switch you to Call 1 and put Call 2 on hold.

Getting Started

This section describes the behavior and startup screens you will see when you plugin and login to your BluStar 8000i.

Plugging In and Starting the BluStar 8000i

When the user plugs in their BluStar 8000i it will turn on automatically and show the login screen. The BluStar 8000i goes through the following startup process when you plug it in.



During startup, the BluStar 8000i checks for any configuration changes or if new firmware updates are available. Once the BluStar 8000i is turned on and ready to go, the login screen appears.

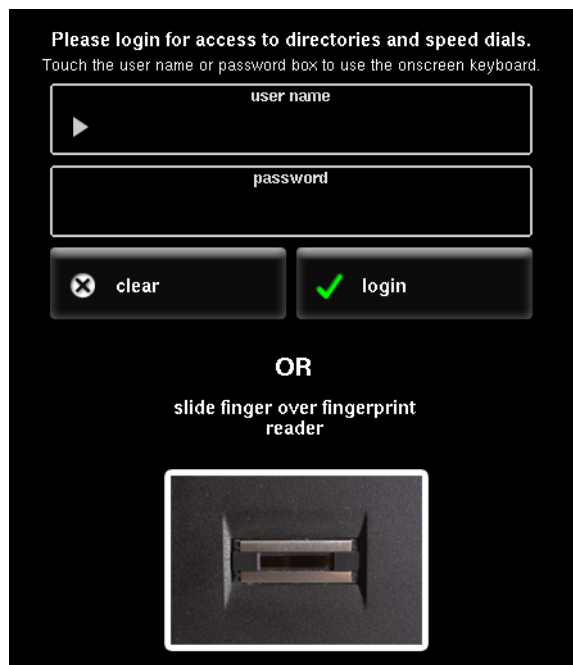
Note:

Users can access certain applications without logging in. Users must login to make calls and access their favorites and other personal settings.

Logging In

In order to make calls, access your personal settings, and use all of the BluStar 8000i applications, you must first login to the terminal. You can login using your **username** and **password** OR by using the **fingerprint reader**.

In order to use the fingerprint reader, you must first login using your username and password and add your fingerprint to your account in the **tools** menu (see [Fingerprint Reader](#) on [page 1-12](#) for more information).



To Log In Using Your Username and Password:

1. On the login window, touch the **user name** button.
2. Use the on-screen keyboard to type in your user name. (Touch **backspace** on the on-screen keyboard or the **clear** button to delete incorrect entries.)
Note:
If you have recently logged in, you can touch the triangle in the user name box. A drop-down menu appears listing recently logged-in users. If your user name appears in the list, touch it to select it.
3. Touch the **password** button and type in your password.
4. Touch **login**.

To Log In Using the Fingerprint Reader:

1. On the login window, slide your finger SLOWLY over the center of the fingerprint reader in a vertical/downward motion.

Login Screens

Once the user touches the **login** button or uses the fingerprint reader, the BluStar 8000i will go through the following login process:



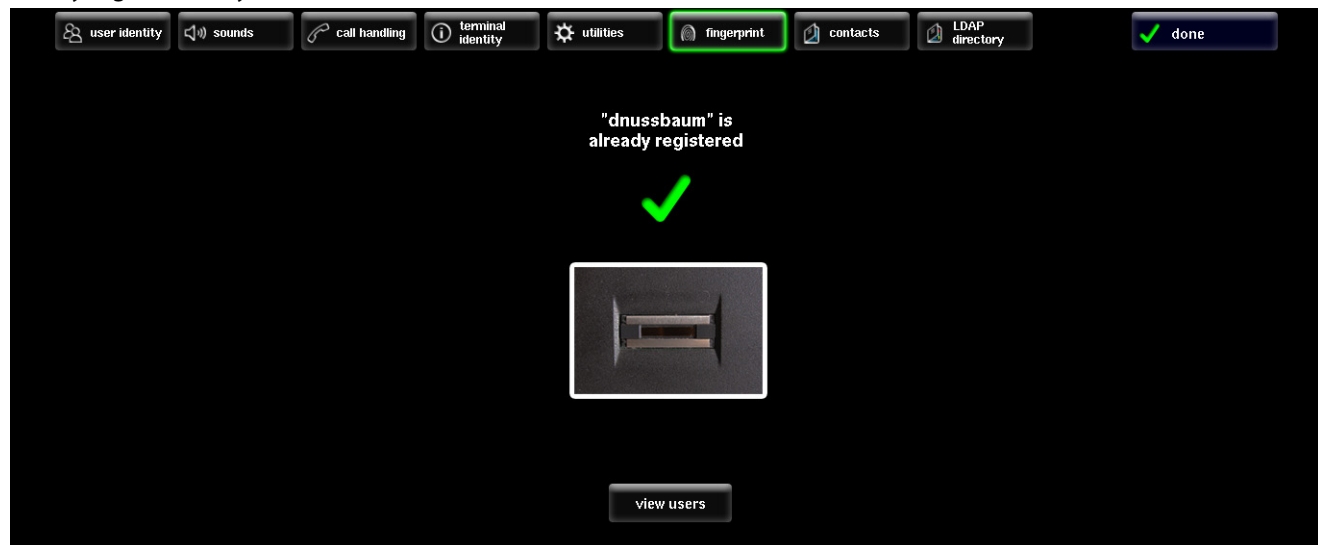
Fingerprint Reader

The biometric fingerprint reader efficiently identifies users and makes hot desking from any BluStar 8000i device an effortless task. A BluStar 8000i terminal can have up to five registered users. If someone wants to use the fingerprint reader to login to a terminal with more than five registered users, then they have to first delete a user on the fingerprint screen in order to add their fingerprint.

The first time you login to the BluStar 8000i you can assign a fingerprint to your account. On the fingerprint screen, you have to login using your username and password to add a new fingerprint.



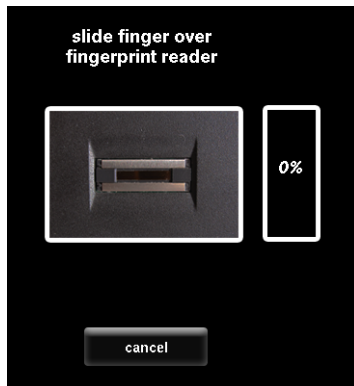
Once you have registered your fingerprint, when you open the fingerprint screen you will see that you have a fingerprint already registered to your account.



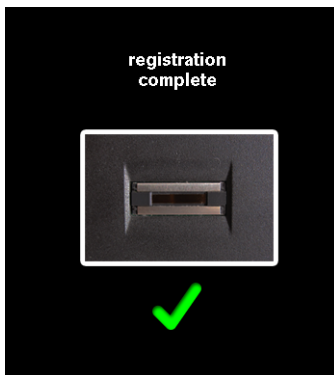
You can select the **view users** button to see how many other users have a saved fingerprint on the terminal.

To Add a Fingerprint:

1. Enter in your login password.
2. Touch **next**.
3. Using the fingerprint reader on the phone (not the image on the screen) swipe your finger SLOWLY in a vertical/downward motion to add a fingerprint.



4. Swipe your finger again.
The status bar increases.
5. Swipe your finger again.
The status bar increases.
6. Swipe your finger again.
Registration is now complete. The status bar increases to 100%.



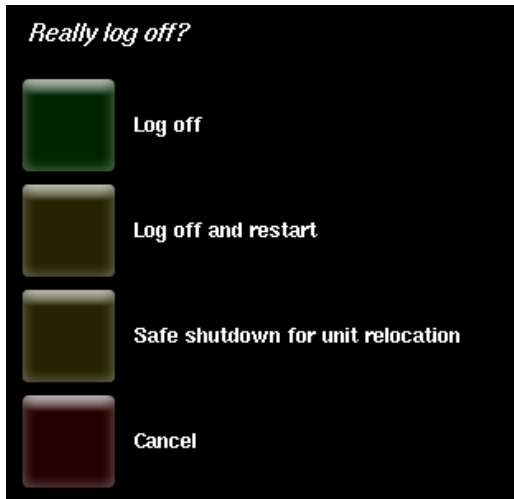
To Delete a Registered User:

1. From the fingerprint screen, touch the **view users** button.
2. Touch the box beside a user and then the **delete selected** button.
The user is removed from the screen.

Logging Off / Restarting

You can log off the BluStar 8000i from the app menu. From the log off screen, you have the option to do the following:

- log off
- log off and restart
- safe shutdown for unit relocation
- cancel



To Log Off:

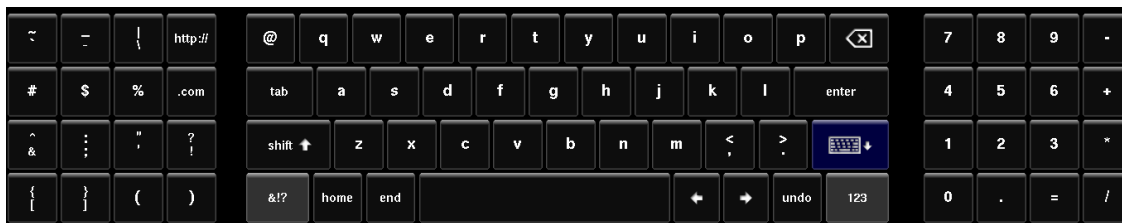
1. Touch the **app menu**.
2. Touch the **log off** button.
3. Touch either:
 - **log off**
 - **log off and restart**
 - **safe shutdown for unit relocation**


Touch Screen Basics

When you use your BluStar 8000i, you will see and interact with several different applications and controls. You can use your fingers to tap buttons, swipe through screens, and scroll through lists. You can tap a button to select it, and tap it again to de-select it. While selected, the button will be outlined in either **green** or **red** (depending on the user interface (UI) element).

On-Screen Keyboard

The touch-sensitive on-screen keyboard essentially functions in the same way as a physical QWERTY keyboard. The keyboard appears automatically when a screen contains editable fields or when you touch an editable field for keyboard input.

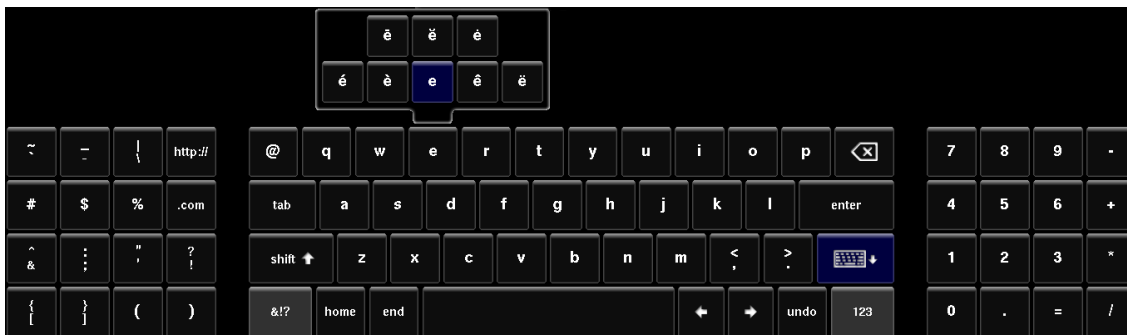


At any time, touching the  button will hide the on-screen keyboard.

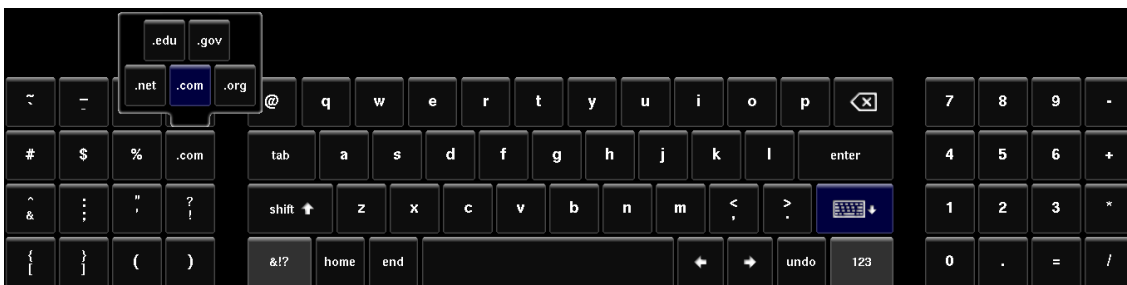
Alternate Functions

Additionally, you can access alternate functions on the on-screen keyboard by pressing and holding any of the specified keys for approximately one second. When you press and hold a key, a menu pops up allowing you to select alternate functions.

For example, as revealed in the image below, when you press and hold the “E” key, additional special characters are available for selection:



When you press and hold the “.com” key, additional alternate functions are available for selection:



The table below shows the keys that support this feature and their corresponding alternate functions:

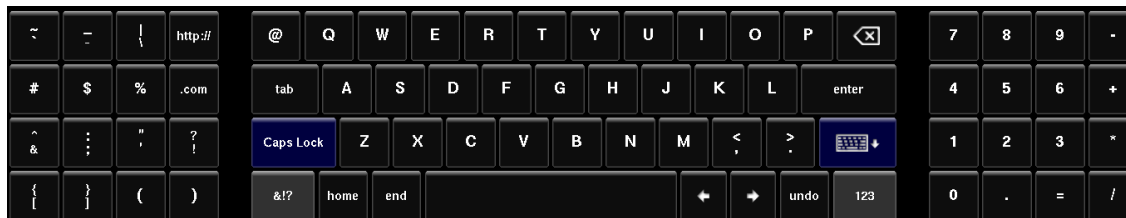
Key	Alternate Function(s)
e	é, è, ê, ë, ê, è, è
E	É, Ê, Ë, Ê, Ê, Ê
s	ß, ś, š
S	Ś, Š
a	á, à, â, ã, ä, å, æ, ā
A	À, Á, Â, Ã, Ä, Å, Æ, Ā
u	ù, ú, û, ü, ũ
U	Ù, Ú, Û, Ü, Ŭ
o	ò, ó, ô, õ, ö, ô, œ, ø
O	Ò, Ó, Ô, Õ, Ö, Õ, Œ, Ø
n	ñ, ñ
N	Ñ, Ñ
c	ç, ć, č
C	Ç, Ć, Č
z	ź, ź, ž
Z	Ż, Ź, Ž
i	ì, í, î, ï, î, î
I	Ì, Í, Î, Ï, Î, Î
y	ÿ
Y	Ÿ
l	ł
.com	.net, .org, .edu, .gov
http://	https://, ftp://, ftp://

Notes:

- For keys that represent two characters (e.g. ?/!, }/}, etc...), pressing and holding the respective key for approximately one second will bring up a menu allowing you to select the secondary character.
- All URL parameters containing special characters found within applicable configuration files must be URL-encoded. Please refer to RFC3986 for further details.

Caps Lock

Pressing and holding the Shift key for approximately one second turns the keyboard into caps lock mode. All characters are displayed as upper case characters and the Shift key is represented as a Caps Lock key indicating caps lock is on.



To turn off caps lock functionality, simply press the Caps Lock key.

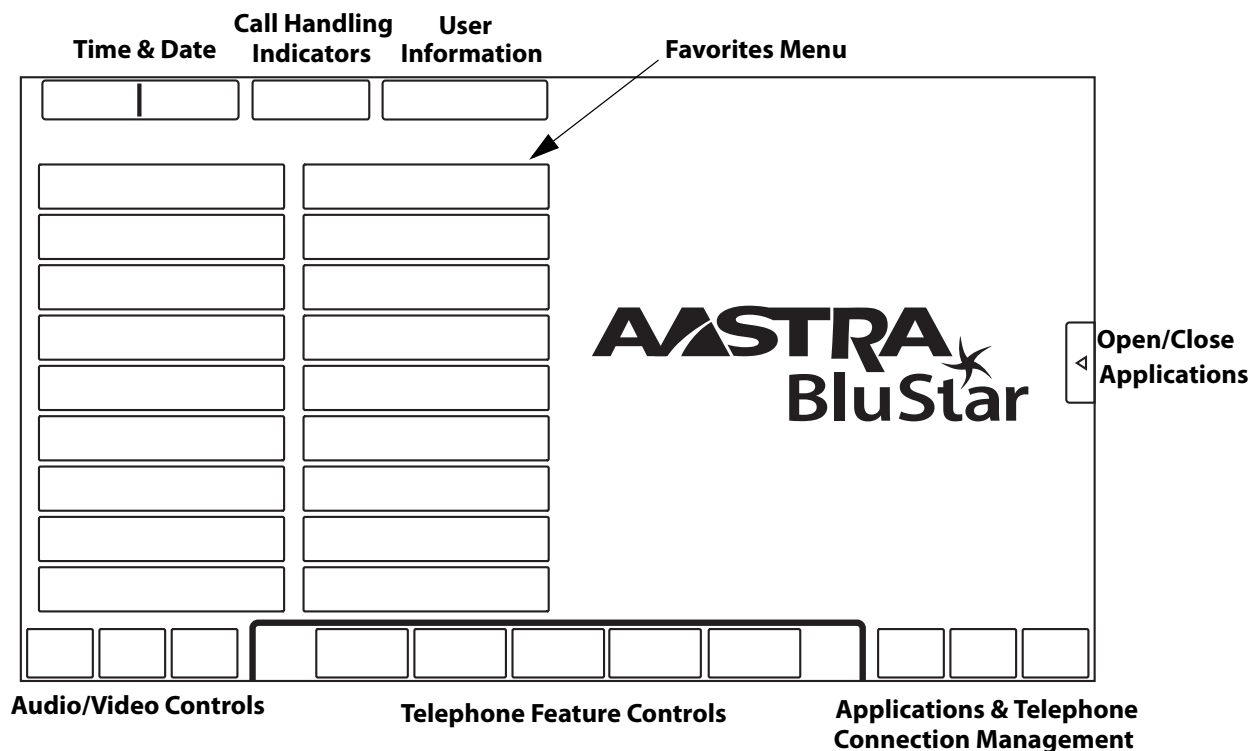
Home Screen

On the home screen you will see the following:

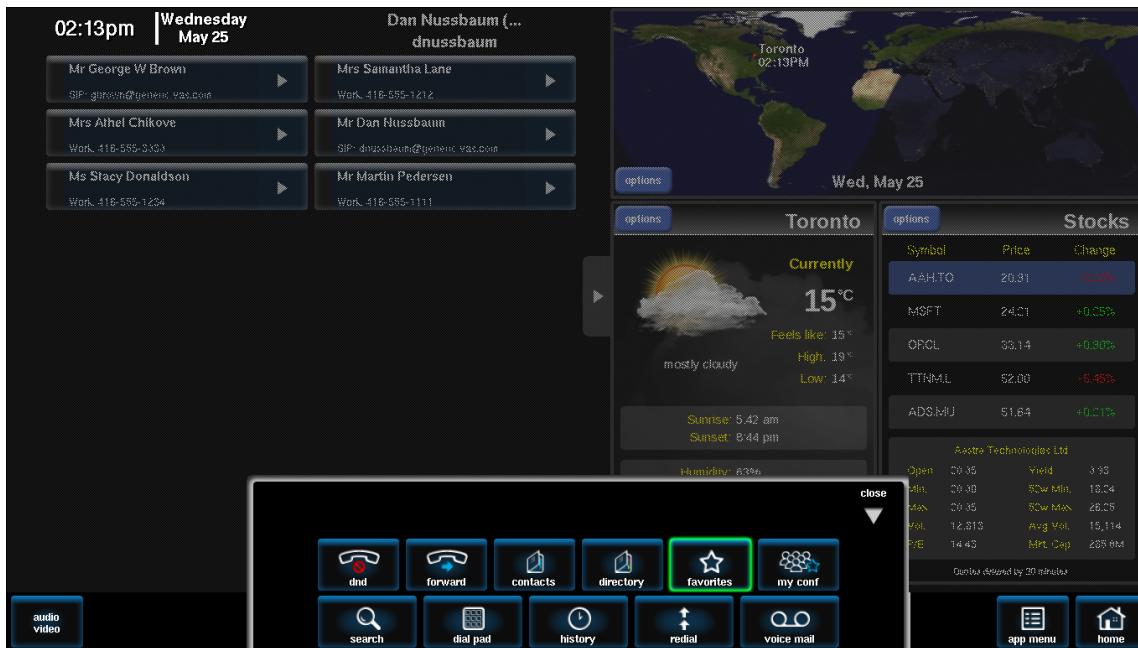
- Time
- Date
- Call handling indicators
- User information
- Favorites menu
- Open/close applications arrow
- Audio/video controls
- Telephone feature controls
- Applications and telephone connection management

Notes:

- The time, date, and user information is set up by the system administrator.
- The call handling indicators (i.e. icons for call forwarding, auto answer, and Do Not Disturb (DND) features) are only displayed when the respective feature is enabled.



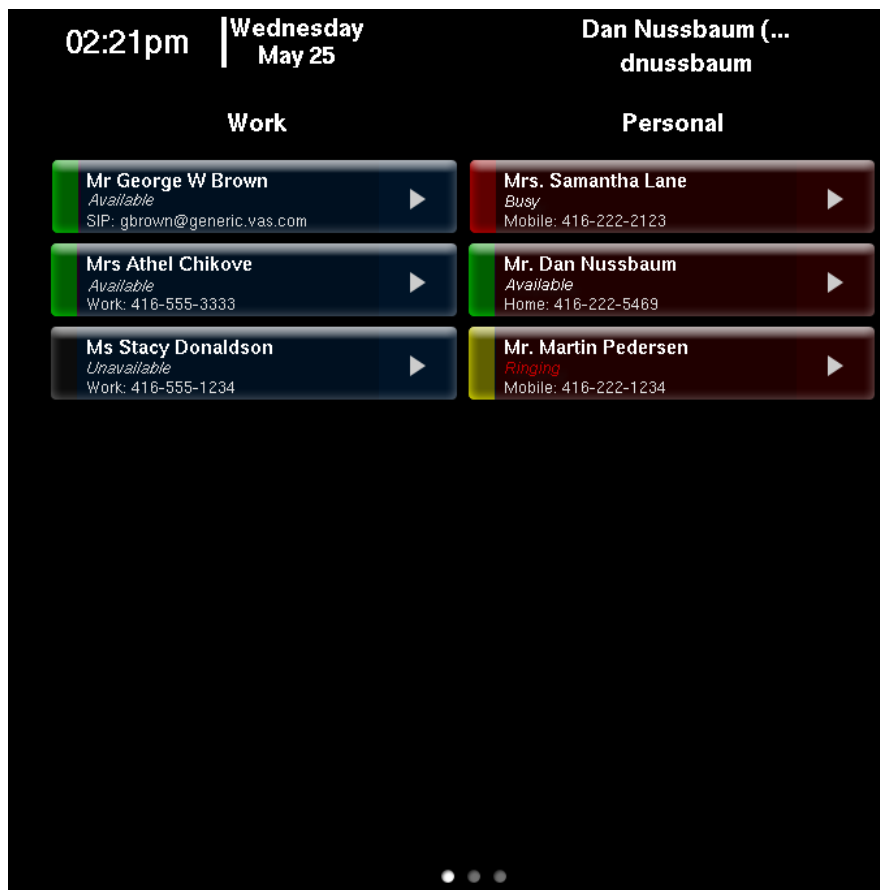
The main screen is greyed out (not the video) when a new (significant) UI element takes focus. For example, you will see the home screen greyed out when you expand the telephone feature controls menu. When you close the menu, you can touch the features and applications on the home screen again.



Favorites Menu

The favorites menu appears automatically on the **home** screen. This menu stores all of your favorite contacts. It acts like a speed dial list, so you can quickly select a contact to call. You can easily add and delete contacts to your favorites menu. You can also monitor contacts for state changes (available [green], ringing [yellow], busy [red], and unavailable [black]) of extensions on the BluStar 8000i (see [Busy Lamp Field \(BLF\)](#) on [page 4-37](#)).

The favorites menu is comprised of three pages each containing 18 cells (for a total of 54 cells) that can be used for either favorite entries or labels. Entries can be color-coded and easily moved to a slot on any of the three pages and unused cells can be edited for use as labels, allowing you to better organize the favorites menu.



Note:

Pages are indicated by the dots located at the bottom of the Favorites Menu. Navigating from page to page is performed by swiping the menu to the left or to the right.

To Open Your Favorites Menu:

1. In the telephone feature controls, touch the **favorites** or the **home** button or press the **home** key on the key panel. The button is outlined in green, indicating that your favorites is open.

To Add a Contact to Your Favorites:

1. In the telephone feature controls, touch the **contacts** button.
2. Touch the arrow on a contact button to open the contact's information screen.
3. Touch the **add to favorites** button.
4. Touch **done**.
You will now see your contact in your favorites menu on the home screen.
Note:
Newly created favorites are placed in the first available slot on the first available page and are highlighted in green.

To Remove a Contact from Your Favorites:

1. In your favorites menu, touch the arrow on a contact button to open up the contact's information screen.
2. Touch **View full contact information**.
3. Touch the **delete favorite** button.
The contact has been removed from your favorites.

To Apply Color-Coding to a Contact in Your Favourites:

1. In your favorites menu, touch the arrow on a contact button to open up the contact's information screen.
2. Touch **View full contact information**.
3. Select a color from the list of available colors under the **favorite** heading.
4. Touch **done**.
You will now see the entry in your favourites menu with the selected color-coding option applied.

To Move Contact Entries Within the Favorites Menu:

1. In your favorites menu, touch and hold the contact entry you wish to move.
The entry will be highlighted in green.
2. Drag and drop the selected contact entry into the desired slot.
You will now see the entry in the desired slot.
Note:
Entries can be placed in a slot on any of the three pages. To move the contact entry to a different page, drag the selected entry to the extreme right or extreme left and drop the entry into the desired slot.

To Create Labels from Unused Cells:

1. In your favorites menu, touch and hold an unused cell (i.e. an empty cell containing no entries).
A cursor will appear allowing you to edit the cell to use as a label.
2. Edit the label by using the on-screen keyboard.
3. Touch **enter**.
You will now see your label in your favorites menu on the home screen. The label can now be moved within the favorites menu in the same fashion as a contact entry.

To Update or Delete a Label:

1. In your favorites menu, touch the cell containing the label you wish to update or delete.
A cursor will appear allowing you to edit the cell to use as a label.
2. Edit the label by using the on-screen keyboard or delete the label using the **backspace** button.
3. Touch **enter**.
The cell will now reflect the changes you have made.

To Go to the Home Screen:

1. Touch the **home** or the **favorites** button
OR
the **home** key.

Adding Apps to the Home Screen

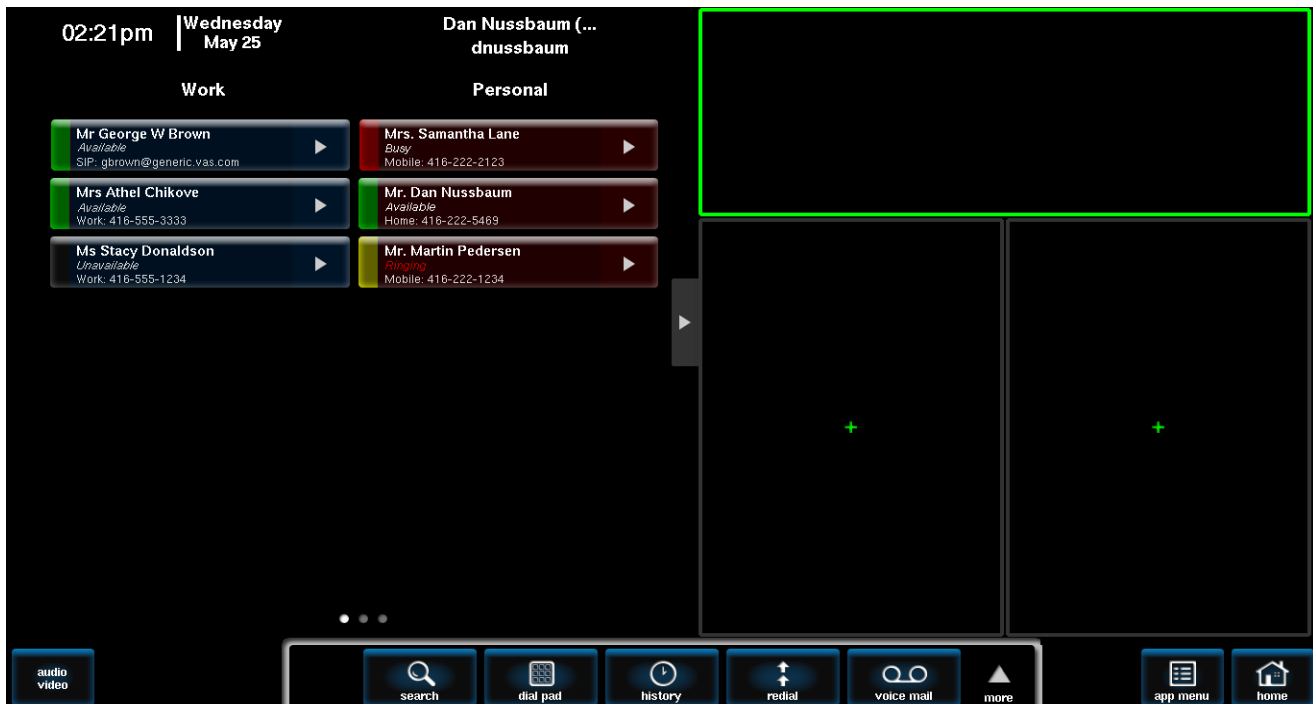
You can customize the applications (apps) that appear on your home screen. The BluStar 8000i has several apps that you can open and/or add to your home screen, and you can display up to three apps at one time. From the app menu, users can easily add or replace apps to one of the three frames on the home screen.

To Add Applications to the Home Screen:

1. Touch the **app menu** button.
2. Touch the app you want to add to the home screen.
3. Touch inside a frame (with or without an app) outlined in green to place the app.

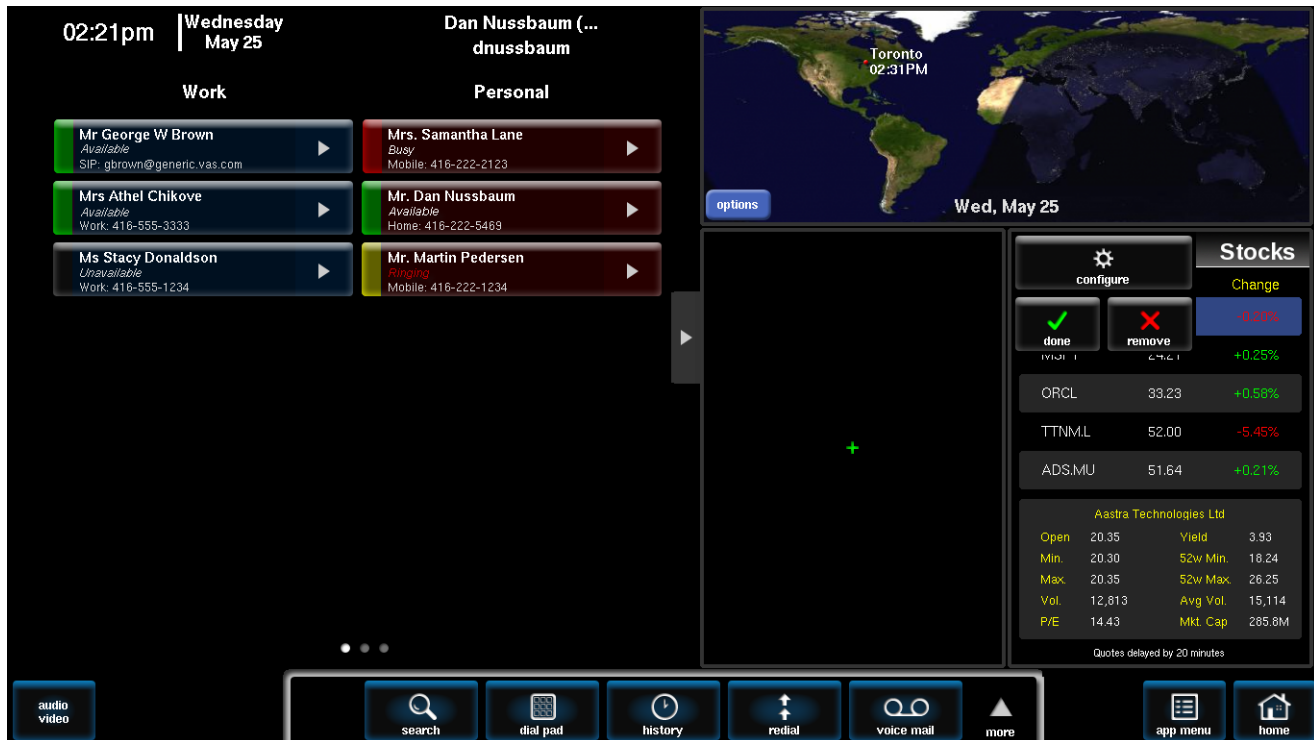
Note:

Only frames that can display a particular app will be outlined in green. For example, the clock app is only designed for the top frame on the home screen, so you won't be able to place it in one of the smaller frames.



To Remove Applications from the Home Screen:

1. Touch the blue **options** button on the top right hand corner of an app.
2. Touch the (-) **remove** button.
You will now see an empty box on the home screen.

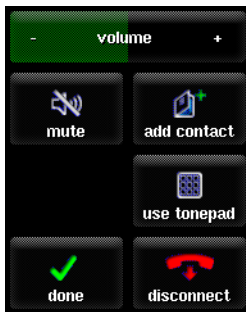
**To Minimize or Maximize the Opened Applications:**

1. Touch the open and close application arrow.



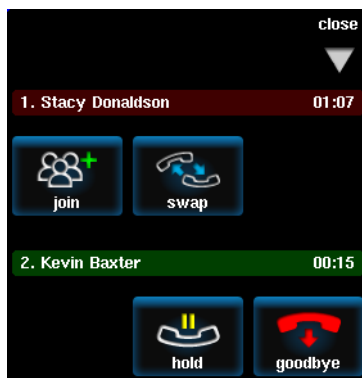
Call Screen

The call screen appears when you are participating in a call. In addition to showing the image(s) and name(s) or number(s) of the people you are talking to, touching the **options** button on a caller's screen will open the **call options menu** where you can:



- Adjust or mute the volume of the party
- Add the party to your address book
- Disconnect the party
- Bring up a tonepad to dial another party

Additionally, the **call appearance bar** provides the call status for the current call, and includes the party's name and elapsed call time.



Lock Screen

For reasons of security, your BluStar 8000i's screen can be locked by touching the **lock screen** button in the app menu, or from a period of system inactivity (configured by your system administrator).

When the preset period of system inactivity is reached, a pop-up window appears informing you that the screen is about to be locked. The window also shows a countdown timer indicating how much time remains before the screen lock is enabled.

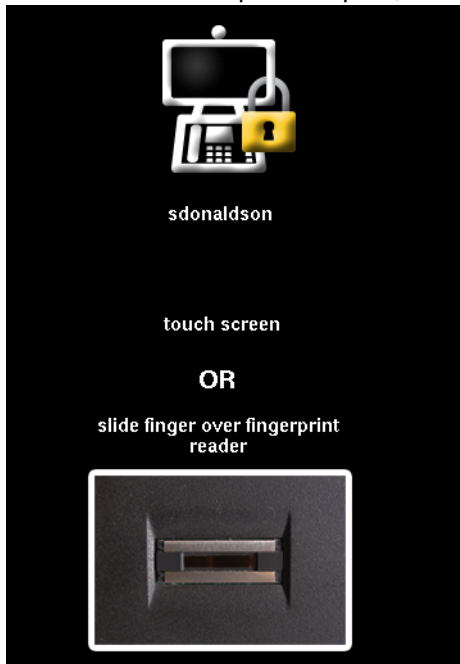
The screen must be locked because of inactivity. Touch to reset.

Screen lock countdown: 2

Note:

Touching the pop-up window aborts the impending screen lock function.

Once the countdown period expires, the terminal locks and displays the following screen:



To Lock the Screen:

1. Touch the **app menu** button.
2. Touch the **lock screen** button.

To Unlock the Screen:

1. Touch anywhere on the screen to enter in your password OR slide your finger over the fingerprint reader in a vertical/downward motion to unlock your terminal.
2. Touch the password box to use the on-screen keyboard.
3. Type in your password. If you make a mistake while entering the password, touch **clear**.

Note:

For security reasons, another user cannot be selected via the username field. The BluStar 8000i system requires that the password of the user who was most recently logged in to the terminal be entered to unlock the terminal.

4. Touch **unlock**.
The terminal unlocks and automatically returns to the screen that displayed before the terminal was locked.

SIP Call Server Installation Information

Description

The setup and installation of the BluStar 8000i in SIP Call Server mode can be done using the configuration files or through the BluStar 8000i UI via the **tools** menu (see [Terminal Identity](#) on [page 4-2](#)).

When the BluStar 8000i is initialized for the first time, Dynamic Host Configuration Protocol (DHCP) is enabled by default. Depending on the type of configuration server setup you have, the BluStar 8000i may download a firmware version automatically, or you may need to download it manually.

Installation Considerations

The following considerations must be made before connecting the BluStar 8000i to the network:

- If you are planning on using dynamic IP addresses, make sure a DHCP server is enabled and running on your network.
- If you are not planning on using dynamic IP addresses, see [Configuring Network Settings Manually](#) on [page 3-6](#) for manually setting up an IP address.
- If you are planning to provide a configuration server by DHCP, see [DHCP](#) on [page 3-3](#) for how to configure the DHCP server.
- On the **terminal identity > advanced** screen in the **tools** menu, the **SIP Call Server** button must be selected and you must enter in the configuration server URL (see [Terminal Identity](#) on [page 4-2](#) for more information). Administrators can do this through the configuration files, manually on the BluStar 8000i UI, or through DHCP options.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Configuration Server Settings](#) on [page A-11](#).

To install the BluStar 8000i terminal, refer to the **Aastra BluStar™ 8000i Desktop Media Phone Quick Start Guide** or the **Aastra BluStar™ 8000i Desktop Media Phone User Guide** for more information.

Installation Requirements

The following are general requirements for setting up and using your BluStar 8000i:

- SIP-based IP PBX system or network installed and running with a SIP account created for the BluStar 8000i
- Ethernet/Fast Ethernet LAN (10/100 Mbps) or Gigabit Ethernet LAN (1000 Mbps)
- Category 5/5e straight through cabling
- Power source

Alert!

For use with included AC/DC adaptor model no. 3A-603DB12 / Pour utiliser avec modèle 3A-603DB12.

Configuration Server Requirements

A basic requirement for setting up the BluStar 8000i is to have a ftp, tftp, http, or https configuration file server (http recommended). On the server you need to have the following files:

aastra.cfg
<model>.cfg
<mac>.cfg

In one of the above files (e.g. the <mac>.cfg file), you must have the BluStar 8000i user configuration URL that specifies where to look for the following file:

<user>.cfg

See [Installing the Configuration Files](#) on [page 2-3](#) for more information.

If HTTP/HTTPS is used to push the <user>.cfg file to the server, then the following two files need to be in a folder specified by the BluStar 8000i user configuration URL:

upload.html
upload_file.php

Notes:

- To obtain these two files, contact Aastra Telecom Support.
- Hot desking will not work when using the HTTP/HTTPS configuration protocol without these two files properly installed on the HTTP configuration server.
- PHP has to be installed on the server and the folder has to allow writing.

Reference

To set the protocol for your configuration server, see [Configuring the Configuration Server Protocol](#) on [page 2-13](#).

Chapter 2

Configuration Server & Files

The BluStar 8000i has specific advanced operational features that you can configure. This chapter describes each feature and provides procedures for configuring a BluStar 8000i to use these features.

This section includes the following information:

- [Configuration Files](#)
 - [Update URL](#)
 - [Configuration Precedence](#)
 - [Installing the Configuration Files](#)
 - [Using the Configuration Files](#)
 - [Encryption](#)
- [Configuration Server](#)
 - [Configuration Server Protocol](#)
 - [Configuration Server Settings](#)
 - [Configuring the Configuration Server Protocol](#)
 - [Configuration Server Redundancy via DNS A Records](#)
 - [Using the Auto-Resync Feature](#)

Configuration Files

A system administrator can enter specific parameters into the configuration files to configure the BluStar 8000i. By default on startup, the BluStar 8000i downloads its configuration files from the configuration server you have set. If the username and password from the login screen is correct, the BluStar 8000i will download its configuration files from the server. The BluStar 8000i supports TFTP, FTP, HTTP, and HTTPS configuration servers.

Note:

For more information on changing the download protocol on your BluStar 8000i, see [Configuring the Configuration Server Protocol](#) on page 2-13.

The configuration files consist of the following files:

- **aastra.cfg** - Contains configuration information that applies to all BluStar and/or all 9000i and 6700i series IP SIP phone devices.
- **<model>.cfg** (e.g. 8000i.cfg) - Contains model specific information.
- **<mac>.cfg** (e.g. 00085D112233.cfg) - Contains configuration information specific to a BluStar device.
- **<user>.cfg** (e.g. jdoe.cfg) - Contains read-only server-related user configuration information that is not configurable through the BluStar 8000i terminal (i.e. sip authentication information, proxy settings, registrar parameters, etc.). The <user>.cfg file can be edited by administrators (even when the user is logged in; however, the changes will not take effect until the next login).
- **<user>_local.cfg** (e.g. jdoe_local.cfg) - Contains hot-desking-related user configuration information that is configurable through the BluStar 8000i terminal (i.e. favorites, call logs, call handling settings, etc.). The <user>_local.cfg file is updated when the local settings on the user's terminal are changed and saved when the user logs off.

Note:

The <user>_local.cfg file must never be edited manually. All user parameters that need to be configured should be defined and edited in the <user>.cfg file only.

In the app menu on the BluStar 8000i UI, users and administrators can view configuration information through the **status** app. Users can click on either **Terminal Configuration** to view configuration information in the aastra.cfg, <model>.cfg, and <mac>.cfg files, or **User Configuration** to view the configuration information in the <user>.cfg file.

Update URL

In order for the BluStar 8000i to download the software, there has to be the “**update url**” parameter in either the <mac>.cfg, <model>.cfg, or aastra.cfg file. It is recommended to have this parameter in the <mac>.cfg file.

For example:

```
update url: ftp://10.55.102.56/aastracfg
```

Note:

All updated system software files provided by Aastra should be placed in the path specified in the “**update url**” parameter.

Reference:

For more information of each configuration file parameter, see [Appendix A “Parameters” on page A-1](#).

For a sample of the configuration files, see [Appendix B “Sample Configuration Files” on page B-1](#).

Configuration Precedence

The BluStar 8000i can accept the following sources of configuration data:

- The configuration server most recently downloaded/cached from the configuration server files: **aastra.cfg/<model>.cfg/<mac>.cfg** (or the aastra.tuz/<model>.tuz/<mac>.tuz encrypted equivalents).
- The BluStar 8000i user configuration URL (“**user config url**” parameter) that specifies where to look for the <user>.cfg (or <user>.tuz encrypted equivalent) file.

Configuration precedence rules are as follows:

- Settings in the <model>.cfg file take precedence over the settings in the aastra.cfg files only.
- Settings in the <mac>.cfg file take precedence over the settings in the <model>.cfg and aastra.cfg files.
- Settings in the <user>.cfg file take precedence over the settings in the <mac>.cfg, <model>.cfg, and aastra.cfg files.
- Settings in the <user>_local.cfg file take precedence over the settings in the <user>.cfg, <mac>.cfg, <model>.cfg, and aastra.cfg files.
- Settings that are locally configured directly through the BluStar 8000i’s UI take precedence over the settings in all of the configuration files.

Notes:

- The BluStar 8000i settings include intelligent default values (therefore an empty configuration file is always the best). Administrators should only set a parameter if they **MUST** control or override that particular setting.
- The internal BluStar 8000i default values can be dynamically adjusted based on network, call, and other conditions and settings.
- If a BluStar 8000i setting value is specified in the configuration file, then this dynamic behavior is disabled for that setting.

Installing the Configuration Files

The following procedure describes how to install the configuration files.

1. If DHCP is disabled, manually enter the configuration server's IP address. For details on manually setting DHCP, see [Configuring Network Settings Manually](#) on [page 3-6](#).
2. On the configuration server, you must have the **aastra.cfg**, **<model>.cfg**, and **<mac>.cfg** files.

Notes:

 - The **<mac>** attribute represents the actual MAC address of your BluStar 8000i (i.e., *00085D112233.cfg*).
 - The terminal's **<mac>** address can be obtained under the **about** app menu.
3. Place the mandatory "user config url" parameter that specifies where to look for the **<user>.cfg** file in either the **aastra.cfg**, **<model>.cfg**, or the **<mac>.cfg** file.

Note:
The "user config URL" parameter supports tftp, ftp, http, https, however only ftp, http and https can be authenticated.
4. Place the "update url" parameter in the **<mac>.cfg** file.

When the BluStar 8000i is booting up, only the **aastra.cfg**, **<model>.cfg**, and **<mac>.cfg** are loaded. The **<user>.cfg** and **<user>_local.cfg** are loaded when the user logs in.

Note:
To login, the BluStar 8000i has to be able to load the **<user>.cfg** file.
5. Restart the BluStar 8000i as described in [Logging Off / Restarting](#) on [page 1-14](#).

Using the Configuration Files

You must use a text-based editing application to open the configuration files (**aastra.cfg**, **<mac>.cfg**, or **<user>.cfg**) to configure the BluStar 8000i.

Note:

The **<user>_local.cfg** file must never be edited manually. All user parameters that need to be configured should be defined and edited in the **<user>.cfg** file only.

Use the following procedure to add, delete, or change parameters and their settings in the configuration files.

Note:

Apply this procedure wherever this guide refers to configuring parameters using the configuration files.



Configuration Files

1. Using a text-based editing application, open the configuration file that you want to configure the parameter in (either **aastra.cfg**, **<model>.cfg**, **<mac>.cfg**, or **<user>.cfg**).
2. Enter the required configuration parameters followed by the applicable value.
For example, in the **<user>.cfg**:
sip user name: 1010
3. Save the changes and close the configuration file.
4. If the parameter requires the BluStar 8000i to be restarted in order for it to take affect, use the **log off** app on the BluStar 8000i UI.

Encryption

An encryption feature for the BluStar 8000i allows service providers the capability of storing encrypted files on their server(s) to protect against unauthorized access and tampering of sensitive information (e.g. user accounts, login passwords, registration information).

Configuration File Encryption Method

Only an administrator can encrypt the configuration files for a BluStar 8000i terminal. Administrators use a password distribution scheme to manually pre-configure or automatically configure the terminals to use the encrypted configuration with a unique key.

From a Microsoft Windows command line, the administrator uses an Aastra-supplied encryption tool called "anacrypt.exe" to encrypt the configuration files.

Note:

Aastra also supplies encryption tools to support Linux platforms (i.e. anacrypt.linux) if required.

This tool processes the plain-text system configuration files (<mac>.cfg, <model>.cfg, and aastra.cfg) as well as the user configuration files (i.e. <user>.cfg and <user>_local.cfg) and creates triple-DES encrypted versions called <mac>.tuz, <model>.tuz, aastra.tuz, <user>.tuz, and <user>_local.tuz. Encryption is performed using a secret password that is chosen by the administrator.

Note:

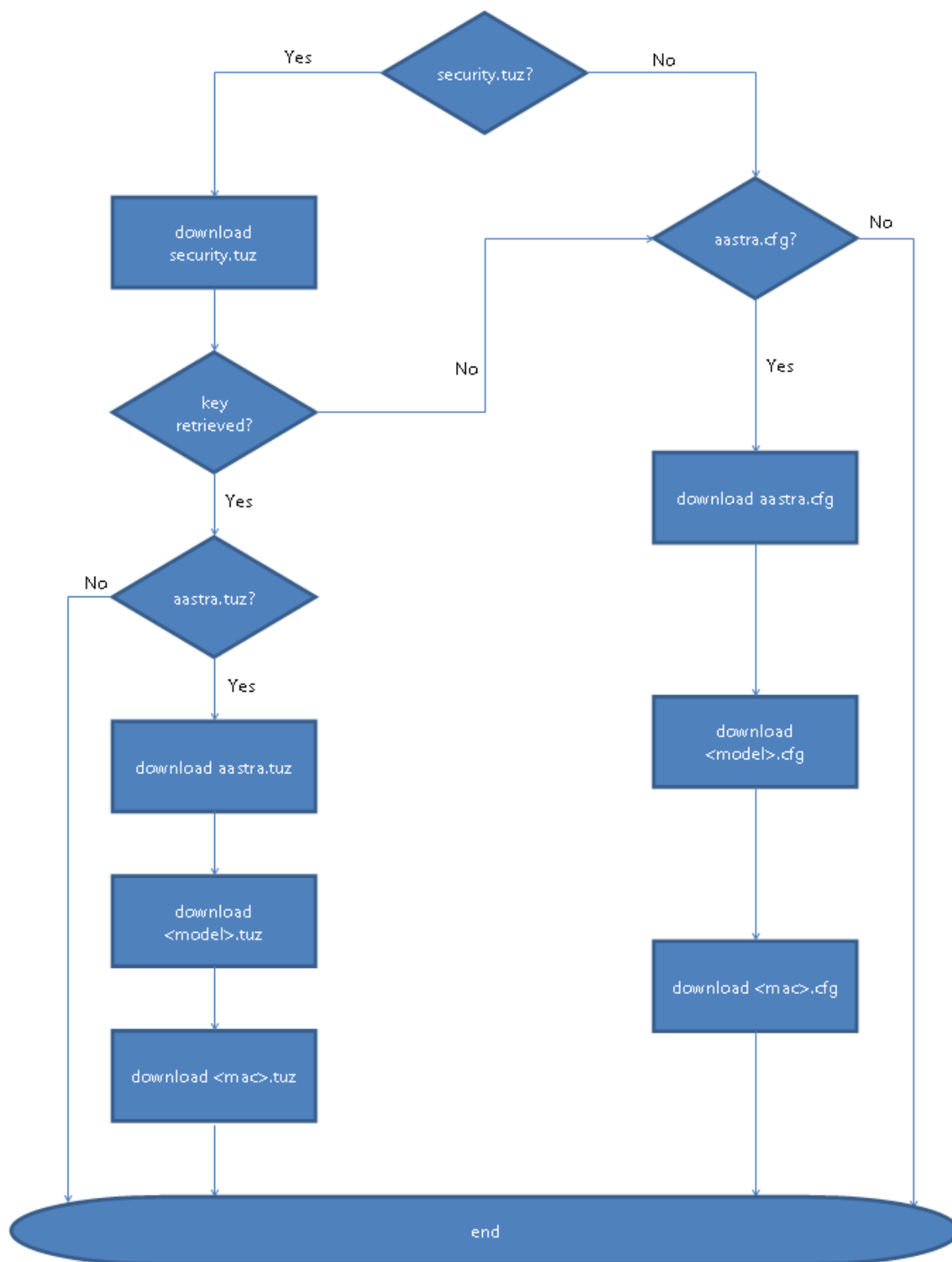
If the system configuration files are located on a different server/directory than the user configuration files, encrypting one set of configuration files does not automatically encrypt other set of configuration files as well.

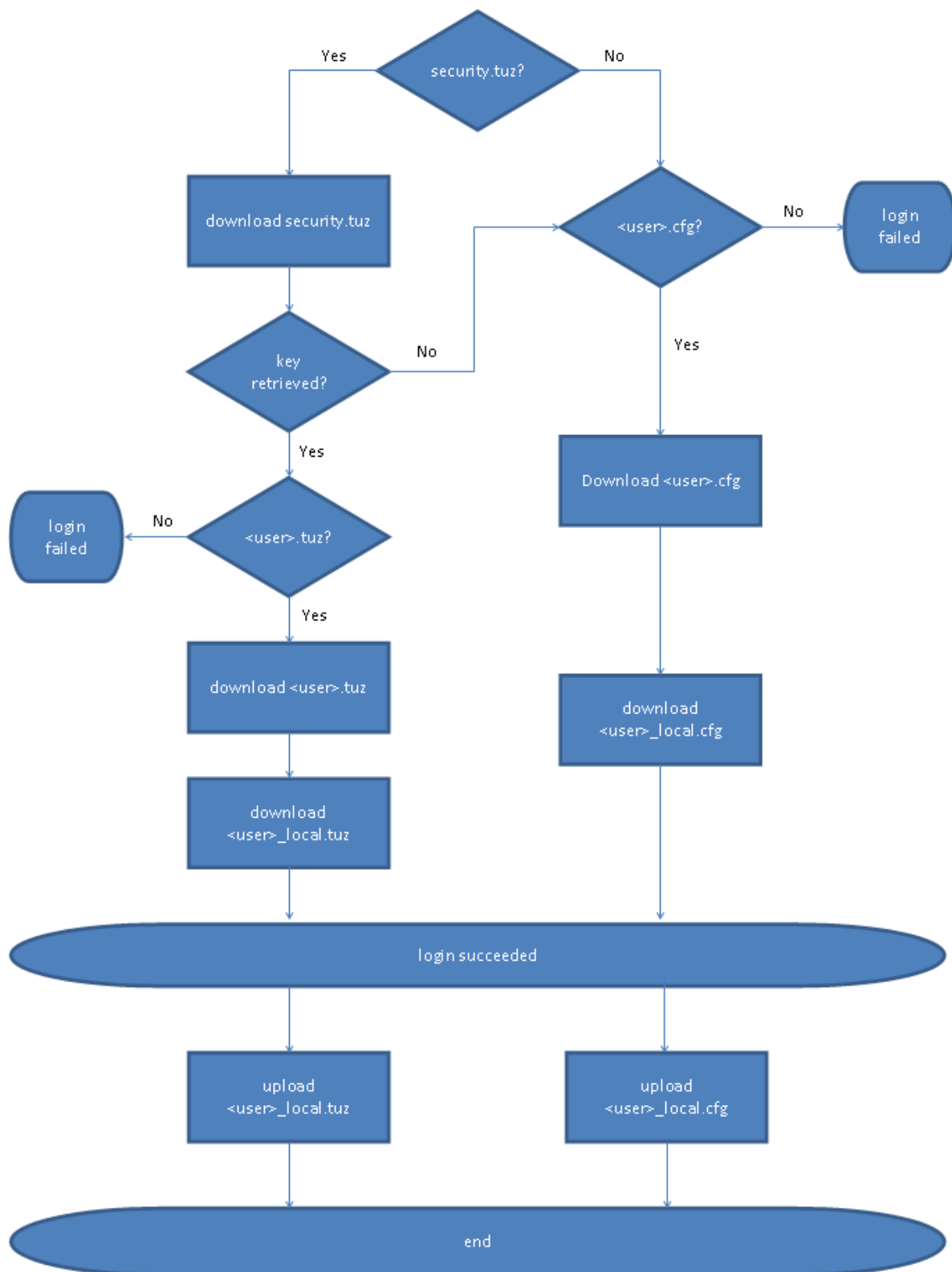
The encryption tool is also used to create additional encrypted tag files called security.tuz, which control the decryption process on the BluStar 8000i. The BluStar 8000i looks for two encryption (i.e. security.tuz) files: one for the system configuration files (during the boot up sequence) and one for the user configuration files (during the login/logout and check-sync processes).

One security.tuz file can be created for use with all configuration files if the system and user configuration files are on the same server/directory. If the system and user configuration files are on separate servers/directories, the same security.tuz file can be shared, but both servers/directories must contain a copy of the same file.

The following flowcharts detail the system configuration download and user configuration download/upload process:

System Configuration Download Process During Boot Sequence



User Configuration Download/Upload During Login/Logout Process

If security.tuz is present on the configuration server during the boot up sequence, the BluStar 8000i downloads it and uses it locally to decrypt the configuration information from the aastra.tuz, <model>.tuz, and <mac>.tuz files. If no security.tuz is present on this configuration server, the BluStar 8000i will download the plain-text aastra.cfg, <model>.cfg, and <mac>.cfg files.

If the user configuration files are located on the same server/directory as the system configuration files and the security.tuz (used at boot up for the system configuration files) is present, the same security.tuz will be used to download and decrypt the <user>.tuz and <user>_local.tuz files at a user login or check-sync and encrypt then upload the <user>_local.tuz file at logout. If no security.tuz is present, the BluStar 8000i will download the plain-text <user>.cfg and <user>_local.cfg files and upload the <user>_local.cfg file at logout.

If the user configuration files are located on a separate user configuration server/directory and a security.tuz file is present, during a user login or check-sync the BluStar 8000i downloads it and uses it locally to decrypt the configuration information from the <user>.tuz and <user>_local.tuz files; this same security.tuz is used to encrypt and upload the <user>_local.tuz file at logout. If no security.tuz is present on this separate user configuration server/directory, the BluStar 8000i will download the plain-text <user>.cfg and <user>_local.cfg files and upload the <user>_local.cfg file at logout.

Notes:

- If the use of encrypted configuration files is enabled (via security.tuz) the .cfg files are ignored and only the encrypted equivalent .tuz files are read.
- Because only the encrypted versions of the configuration files need to be stored on the server(s), no plain-text configuration or passwords are sent across the network, thereby ensuring security of the configuration data.
- To make changes to the configuration files, the administrator must save the original files.

Three versions of encryption are available (i.e. v1, v2, and v3) for the BluStar 8000i configuration files each utilizing different encryption routines.

Note:

Configuration files that are encrypted using v3 encryption can only be decoded by BluStar 8000i terminals on Release 4.1.1 (and above). Terminals with v3-encrypted configuration files will lose the ability to decode the files (and in turn will lose all previously configured settings) if they are downgraded to any firmware release below 4.1.1.

Additionally MAC-specific encryption is also available as an option. MAC-specific encryption prevents unauthorized parties from reading or writing the contents of the <mac>.tuz file. It also provides the following:

- Prevents users from using the <mac>.tuz file that does not match the user's terminal MAC address.
- Renders the <mac>.tuz file invalid if the user renames the file.

Encrypting Configuration Files

Use the following procedure to encrypt the BluStar 8000i configuration files:

1. Obtain the anacrypt encryption tool (anacrypt.exe) from your Aastra representative.
1. Open a command line window application (i.e., DOS window).
2. At the prompt, enter **anacrypt.exe** and press <Return>.
3. Enter a command utilizing the details provided in the help screen.

```
C:\> anacrypt.exe -h
Provides encryption of the configuration files used for the
family of Aastra IP phones.

Copyright (c) 2005-2012, Aastra Technologies, Ltd.

Usage:
anacrypt {infile.cfg|-d <dir>} [-p password] [-m] [-i] [-v] [-h]
```

Anacrypt Switch	Description
{infile.cfg -d <dir>}	Specifies that all .cfg files in <dir> should be encrypted.
[-p password]	Specify password used to generate keys.
-m	Generate MAC.tuz files that are terminal specific.
-v1	Specifies the version of encryption that the anacrypt tool uses.
-v2	(Default) Specifies the version of encryption that the anacrypt tool uses.
-v3	(Enhanced security version) Specifies the version of encryption that the anacrypt tool uses.
-i	Generate security.tuz file.
-h	Show the help screen.

Examples

The following examples illustrate the use of the anacrypt.exe file.

Example 1

Generating a security.tuz file with password 1234abcd (using the v3 encryption process):

```
C:\>anacrypt -i -p 1234abcd -v3
```

Example 2

Generating a security.tuz file with password 1234abcd (using the v2 encryption process):

```
C:\>anacrypt -i -p 1234abcd
```

or

```
C:\>anacrypt -i -p 1234abcd -v2
```

Example 3

Generating a security.tuz file with password 1234abcd (using the v1 encryption process):

```
C:\>anacrypt -i -p 1234abcd -v1
```

Example 4

Encrypting a single aastra.cfg file with password 1234abcd (using the v3 encryption process):

```
C:\>anacrypt aastra.cfg -p 1234abcd -v3
```

Example 5

Encrypting a <mac>.cfg file with password 1234abcd (using the v3 encryption process):

```
C:\>anacrypt 00085d000000.cfg -p 1234abcd -v3
```

Example 6

Encrypting a <mac>.cfg file with password 1234abcd using MAC encryption (using the v3 encryption process):

```
C:\>anacrypt 00085d000000.cfg -m -p 1234abcd -v3
```

Example 7

Encrypting all cfg files in C:\data with password 1234abcd using MAC encryption and generating a security.tuz file at the same time (using the v3 encryption process):

```
C:\>anacrypt -d C:\data -p 1234abcd -m -i -v3
```

Example 8

Encrypting all cfg files in C:\data with password 1234abcd and generating a security.tuz file at the same time (using the v3 encryption process):

```
C:\>anacrypt -d C:\data -p 1234abcd -i -v3
```

Configuration Server

Configuration Server Protocol

You can download new versions of software and configuration files from the configuration server to the BluStar 8000i using any of the following types of protocols:

- TFTP
- FTP
- HTTP
- HTTPS

For each protocol, you can specify the path for which the configuration files are located on the server.

For HTTP and HTTPS you can also specify the port number to use for downloading the BluStar 8000i configuration files.

For FTP you can configure a username and password that are authenticated by the FTP server.

Note:

The configuration server can be configured from configuration files (see [Configuration Server Settings](#) on page 2-10), DHCP (see [DHCP](#) on page 3-3), and from the BluStar 8000i UI (see [Terminal Identity](#) on page 4-2).

When loading the .cfg/.tuz and .csv files, FTP uses the username and password from the FTP URL in the configuration file. If a password is not provided, it tries anonymous access.

Configuration Server Settings

The configuration server stores the configuration files and the software to perform software upgrades to the BluStar 8000i. A system administrator can configure the parameters listed in the table below for the configuration server set for loading the aastra.cfg, <model>.cfg, and <mac>.cfg files (or .tuz encrypted equivalents). For loading the user configuration files, the “**user config url**” parameter is used.

Parameters in Configuration Files	Description
Download Protocol Setting	
download protocol	<p>Protocol to download configuration files. Valid values are:</p> <p>TFTP FTP HTTP HTTPS For example, download protocol: HTTP</p> <p>For DHCP to automatically populate the IP address or domain name for the download servers, your DHCP server must support Option 66. For more information, see DHCP on page 3-3.</p>
download timeout	<p>Specifies the overall timeout (seconds) for downloading the configuration files (aastra.cfg, <model>.cfg, and <mac>.cfg [or .tuz encrypted equivalents]).</p> <p>For example, download timeout: 40</p>
download connect timeout	<p>Complements the “download timeout” parameter. Whereas the “download timeout” parameter is used to specify the timeout for downloading the configuration files, the “download connect timeout” parameter specifies the amount of time allowed (in seconds) for the BluStar 8000i to connect to the configuration server.</p> <p>For example, download connect timeout: 20</p>

Parameters in Configuration Files	Description
pbx mode	<p>Specifies the call server mode for the BluStar 8000i (SIP Call Server or BluStar Application Server). For example, lpbx mode: 1</p> <p>Note: If configuration server details are being set by the DHCP server, ensure that the locked parameter “!pbx mode: 1” is added to the aastra.cfg file for SIP Call Server mode (see Configuration Server Settings on page A-11 for parameter details). As the default server type is locally set to BluStar Application Server on the BluStar 8000i and the local terminal settings take precedence over the configuration files, failure to lock the “pbx mode” parameter may cause the BluStar 8000i to boot into BluStar Application Server mode upon a restart.</p>
update url	<p>The URL to upgrade the BluStar 8000i software. For example, update url: ftp://10.55.102.56/aastracfg</p> <p>Notes:</p> <ul style="list-style-type: none"> • The software upgrade process will be initiated on the first reboot after the parameter has been modified. • This parameter does not support TFTP.
user config url	<p>The URL to load the user configuration files. For example, user config url: http://10.55.102.56/aastracfg/usercfg</p> <p>Note: The “user config url” parameter supports tftp, ftp, http, https, however only ftp, http, and https can be authenticated.</p>
enable user configuration server redirection	<p>Used to enable HTTP(S) redirection when downloading the user.cfg and downloading/uploading the user_local.cfg files in such cases where the user configuration files are located on the SIP call server node hosting the subscription. For example, enable user configuration server redirection: 1</p>
telephone integration url	<p>The URL (http or https) that the BluStar 8000i calls to perform SIP Call Server integration. This is done during the login sequence and later to activate/deactivate server side feature integration, such as DND, Call Forward, etc. For example, telephony integration url: http://myserver.com/integration.php</p>
telephony integration use login credentials	<p>By default the BluStar 8000i uses SIP credentials to authenticate (digest method) to the SIP Call Server integration server. Enabling this configuration parameter makes the BluStar 8000i use the user login/password instead. For example, telephony integration use login credentials: 1</p>
telephony integration needs sip registration	<p>Used by the telephony integration API to indicate to the software if SIP registration is needed before sending a user command via the API. When enabled, the BluStar 8000i checks the extension registration status before sending an API command. If the extension is not registered, an error message is displayed. For example, telephony integration needs sip registration: 1</p>
tftp server	<p>The TFTP server’s IP address. If DHCP is enabled and the DHCP server provides the information, this field is automatically populated. Use this parameter to change the IP address or domain name of the TFTP server. This will become effective after this configuration file has been downloaded into the BluStar 8000i. For example, tftp server: 192.168.0.130</p> <p>Note: For DHCP to automatically populate this parameter, your DHCP server must support Option 66.</p>
tftp path	<p>Specifies the path name for which the configuration files reside on the TFTP server for downloading to the BluStar 8000i. For example, tftp path: configs\tftp</p> <p>Note: Enter the path name in the form folderX\folderX. For example, blustar8000i\configfiles.</p>
ftp server	<p>The FTP server’s IP address or network host name. This will become effective after this configuration file has been downloaded into the BluStar 8000i. For example, ftp server: 192.168.0.131</p> <p>Optional: You can also assign a username and password for access to the FTP server. See the “ftp username” and “ftp password” parameters for setting these credentials.</p>
ftp path	<p>Specifies the path name for which the configuration files reside on the FTP server for downloading to the BluStar 8000i. For example, ftp path: configs\ftp</p> <p>If the BluStar 8000i’s configuration and software files are located in a sub-directory beneath the server’s root directory, the relative path to that sub-directory should be entered in this field.</p>

Parameters in Configuration Files	Description
ftp username	<p>The username to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the BluStar 8000i. For example, ftp username: aastraconfig</p> <p>The BluStar 8000i supports usernames containing dots (".").</p>
ftp password	<p>The password to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the BluStar 8000i. For example, ftp password: 1234</p>
http server	<p>The HTTP server's IP address. This will become effective after this configuration file has been downloaded into the BluStar 8000i. For example, http server: 192.168.0.132</p> <p>Optional: You can also assign an HTTP relative path to the HTTP server. See the next parameter (http path).</p>
http path	<p>Specifies the path name for which the configuration files reside on the HTTP server for downloading to the IP BluStar 8000i. For example: http path: blustar/1</p> <p>If the BluStar 8000i's configuration and firmware files are located in a sub-directory beneath the server's HTTP root directory, the relative path to that sub-directory should be entered in this field.</p>
http port	<p>Specifies the HTTP port that the server uses to load the configuration to the BluStar 8000i over HTTP. The default port is 80. For example: http port: 1025</p>
https sever	<p>The HTTPS server's IP address. This will become effective after this configuration file has been downloaded into the BluStar 8000i. For example: https server: 192.168.0.143</p> <p>Optional: You can also assign an HTTPS relative path to the HTTPS server. See the next parameter (https path).</p>
https path	<p>Specifies the path name for which the configuration files reside on the HTTPS server for downloading to the IP BluStar 8000i. For example: https path: blustar/1</p> <p>If the BluStar 8000i's configuration and firmware files are located in a sub-directory beneath the server's HTTPS root directory, the relative path to that sub-directory should be entered in this field.</p>
https port	<p>Specifies the HTTPS port that the server uses to load the configuration to the BluStar 8000i over HTTPS. The default port is 80. For example: https port: 1025</p>
Auto-Resync Setting	
auto resync mode	<p>Enables and disables the BluStar 8000i to be updated automatically once a day at a specific time in a 24-hour period. This parameter works with TFTP, FTP, and HTTP servers.</p> <p>Notes:</p> <ul style="list-style-type: none"> Any changes made using the BluStar 8000i are not overwritten by an auto-resync update. Auto-resync affects the configuration files only. The resync time is based on the local time of the BluStar 8000i. If the BluStar 8000i is in use (not idle) at the time of the resync check, the reboot occurs when the BluStar 8000i becomes idle. The automatic update feature works with both encrypted and plain text configuration files. <p>For more information, see Using the Auto-Resync Feature on page 2-13.</p>

Parameters in Configuration Files	Description
auto resync time	<p>BluStar 8000i to be automatically updated. This parameter works with TFTP, FTP, and HTTP servers.</p> <p>Notes:</p> <ul style="list-style-type: none"> • The resync time is based on the local time of the BluStar 8000i. • The value of 00:00 is 12:00 A.M. • When entering a value for this parameter using the configuration files, the value can be entered using minute values from 00 to 59 (for example, the auto resync time can be entered as 02:56). <p>For more information, see Using the Auto-Resync Feature on page 2-13.</p>
auto resync max delay	<p>Specifies the maximum time, in minutes, the BluStar 8000i waits past the scheduled time before starting a checksync.</p> <p>For more information, see Using the Auto-Resync Feature on page 2-13.</p>

Configuring the Configuration Server Protocol

Use the following procedure to configure the configuration server protocol.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Configuration Server Settings](#) on [page A-11](#).

Configuration Server Redundancy via DNS A Records

The BluStar 8000i sends a DNS query and in the DNS response, it accepts the first server IP address and contacts that server, ignoring any additional IP addresses in the response. This allows service providers to manage load balancing (via the DNS server putting different records first on each request), but does not provide redundancy.

Using the Auto-Resync Feature

The auto-resync feature on the BluStar 8000i allows an administrator to enable the BluStar 8000i to be updated automatically once a day at a specific time in a 24-hour period if the files on the server have changed. This feature works with TFTP, FTP, HTTP, and HTTPS servers. An administrator can enable this feature using the configuration files (aastra.cfg, <model>.cfg, and <mac>.cfg).

In the configuration files, you can set the following parameters:

- **“auto resync mode”** - Determines whether the configuration server automatically updates the BluStar 8000i's configuration files or disables automatic updates. This parameter works with TFTP, FTP, HTTP, and HTTPS servers.
- **“auto resync time”** - Sets the time of day in a 24-hour period for the BluStar 8000i to be automatically updated. This parameter works with TFTP, FTP, HTTP and HTTPS servers.
- **“auto resync max delay”** - Specifies the maximum time, in minutes, the BluStar 8000i waits past the scheduled time before starting a checksync. Setting the **“auto resync max delay”** (Maximum Delay) parameter can greatly reduce the load placed on the configuration server when downloading configurations.

Notes:

- Any changes made using the BluStar 8000i are not overwritten by an auto-resync update. Auto-resync affects the configuration files only.
- If the BluStar 8000i is in use (not idle) at the time of the resync check, the reboot occurs when the BluStar 8000i becomes idle.
- The resync time is based on the local time of the BluStar 8000i.
- The automatic update feature works with both encrypted and plain text configuration files.

Enabling Auto-Resync Using the Configuration Files

Use the following procedure to configure automatic updates of the BluStar 8000i firmware, configuration files, or both.

**Configuration Files**

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Configuration Server Settings](#) on [page A-11](#).

Chapter 3

Configuring Network Features

This chapter provides the information required to configure [Network Settings](#) and [SIP Account Settings](#) on the BluStar 8000i via the configuration files.

Network Settings

This section describes the following information:

- [Basic Network Settings](#)
- [DHCP](#)
- [Configuration Server Download Precedence](#)
- [DNS Caching](#)
- [Configuring Network Settings Manually](#)
- [Configuring LAN and PC Port Negotiation](#)
- [Network Time Servers](#)
- [Type of Service \(ToS\), Quality of Service \(QoS\), and DiffServ QoS](#)
- [Virtual Local Area Network \(VLAN\)](#)
- [Virtual Private Network \(VPN\)](#)
- [SIP Account Settings](#)

Basic Network Settings

If Dynamic Host Configuration Protocol (DHCP) is enabled, the BluStar automatically configures all of the network settings. If the BluStar 8000i cannot populate the network settings, or if DHCP is disabled, you can set the network options manually.

Parameters in Configuration Files	Description
dhcp	Enables or disables DHCP. Enabling DHCP populates the required network information. The DHCP server provides the network information that the BluStar 8000i requires. If the BluStar 8000i is unable to get any required information, then you must enter it manually. DHCP populates the following network information: IP Address, Subnet Mask, Gateway, Domain Name Servers (DNS), HTTP HTTPS, TFTP, and FTP servers, and time servers. For example, dhcp: 1 For more information, see DHCP on page 3-3 .
ip	IP address of the BluStar 8000i. To assign a static IP address, disable DHCP. For example, ip: 192.168.0.25 For more information, see Configuring Network Settings Manually on page 3-6 .
subnet mask	Subnet mask defines the IP address range local to the BluStar 8000i. To assign a static subnet mask, disable DHCP. For example, subnet mask: 255.255.255.224 For more information, see Configuring Network Settings Manually on page 3-6 .

Parameters in Configuration Files	Description
default gateway	<p>The IP address of the network's gateway or default router IP address. To assign a static Gateway IP address, disable DHCP.</p> <p>For example, default gateway: 192.168.0.1</p> <p>For more information, see Configuring Network Settings Manually on page 3-6.</p>
dns1	<p>Primary domain name server (DNS) IP address. For any of the IP address settings on the BluStar 8000i, a domain name value can be entered instead of an IP address. With the help of the domain name servers, the domain names for such parameters can then be resolved to their corresponding IP addresses.</p> <p>For example, dns1: 192.168.0.5</p> <p>To assign static DNS addresses, disable DHCP.</p> <p>If a host name is configured on the BluStar 8000i, you must also set a DNS.</p> <p>For more information, see Configuring Network Settings Manually on page 3-6.</p>
dns2	<p>A service that translates domain names into IP addresses. To assign static DNS addresses, disable DHCP.</p> <p>For example, dns2: 192.168.0.6</p> <p>For more information, see Configuring Network Settings Manually on page 3-6.</p>
ethernet port 0	<p>The send (TX) and receive (RX) method to use on Ethernet port 0 to transmit and receive data over the LAN.</p> <p>For example, ethernet port 0: 3 (half-duplex, 10Mbps)</p> <p>For more information on configuring the LAN and PC port negotiation, see Configuring LAN and PC Port Negotiation on page 3-7.</p>
time server disabled	<p>This parameter allows you to enable or disable the Network Time Server (NTP) to set the time on the BluStar 8000i. This parameter affects the "time server1", "time server2", and "time server3" parameters. Setting this parameter to '0' allows the use of the configured Time Server(s). Setting this parameter to '1' prevents the use of the configured Time Server(s).</p> <p>For more information on this feature, see Network Time Servers on page 3-8.</p>
time server1	<p>This parameter allows you to set the IP address of Time Server 1 in dotted decimal format.</p> <p>For more information on this feature, see Network Time Servers on page 3-8.</p>
time server2	<p>This parameter allows you to set the IP address of Time Server 2 in dotted decimal format.</p> <p>For more information on this feature, see Network Time Servers on page 3-8.</p>
time server3	<p>This parameter allows you to set the IP address of Time Server 3 in dotted decimal format.</p> <p>For more information on this feature, see Network Time Servers on page 3-8.</p>

DHCP

The BluStar 8000i is capable of querying a DHCP server, allowing a network administrator a centralized and automated method of configuring various network parameters for the BluStar 8000i.

If DHCP is enabled, the BluStar 8000i requests the following network information:

- Subnet Mask
- Gateway (i.e. router)
- Domain Name Server (DNS)
- Network Time Protocol Server
- IP Address
- TFTP Server
- TFTP Path
- FTP Server
- FTP Path
- HTTP Server
- HTTP Path
- HTTP Port
- HTTPS Server
- HTTPS Path
- HTTPS Port

The network administrator chooses which of these parameters (if any) are supplied to the BluStar 8000i by the DHCP server. The administrator must configure the BluStar 8000i manually to provide any required network parameters not supplied by the DHCP server.

Notes:

- For DHCP to automatically populate the IP address or domain name for the TFTP, FTP, HTTP, or HTTPS configuration servers, your DHCP server must support download protocols according to RFC2131 and RFC1541 for Options 43, 160, 159, and 66.
- If configuration server details are being set by the DHCP server, ensure that the locked parameter “**!pbx mode: 1**” is added to the `aastra.cfg` file for SIP Call Server mode (see [Configuration Server Settings](#) on [page A-11](#) for parameter details). As the default server type is locally set to BluStar Application Server on the BluStar 8000i and the local terminal settings take precedence over the configuration files, failure to lock the “**pbx mode**” parameter may cause the BluStar 8000i to boot into BluStar Application Server mode upon a restart.

To Enable/Disable DHCP:

Use the following procedure to enable/disable DHCP on the BluStar 8000i using the configuration files.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Network Settings](#) on [page A-4](#).

DHCP Options 66, 60, and 43 Server Configuration

Option 66

The BluStar 8000i supports download protocols according to RFC2131 and RFC1541 (TFTP, FTP, HTTP, HTTPS) to support DHCP option 66. Option 66 is part of the DHCP offer message that the DHCP server generates to tell the BluStar 8000i which configuration server it should use to download new firmware and configuration files.

For DHCP to automatically populate the IP address or domain name for the servers, your DHCP server must support Option 66. Option 66 is responsible for forwarding the server's IP address or domain name to the BluStar 8000i automatically. If your DHCP server does not support Option 66, you must manually enter the IP address or domain name for your applicable configuration server into your BluStar 8000i configuration.

Option 60 and 43

The BluStar 8000i also supports Option 60 and Option 43 as per RFC 2132.

Option 60 (Vendor Class Identifier) provides the DHCP server with a unique identifier for each BluStar model. This enables a system administrator to send the BluStar 8000i a customized server configuration in Option 43.

For example, for model 8000i, the identifier value would be the following:

Model	Identifier Value
8000i	AastraBluStar8000i

The system administrator can use the Vendor Class Identifier to send the BluStar a customized Server Configuration in Option 43 (vendor-specific information).

Note:

If the BluStar 8000i receives the server configuration from both DHCP Option 66 and Option 43, Option 43 takes precedence over Option 66.

Using Option 43 to Customize the BluStar 8000i

A system administrator can customize the BluStar 8000i in the network by enabling sub-option 2 to send configuration server information using one of the following formats:

Sub-Option Code	Protocol	Format
2	HTTP	http://<server>/<path>
2	HTTPS	https://<server>/<path>
2	TFTP	tftp://tftpserver
2	FTP	ftp://user:password@ftpserver

Using Option 12 Hostname

If you set the BluStar 8000i to use DHCP Option 12, it automatically sends this option to the configuration server. This option specifies the hostname (name of the client). The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character set restrictions.

Notes:

- The hostname of [<model><MAC address>] automatically populates the field on initial startup of the BluStar 8000i.
- If the configuration server sends the hostname back to the BluStar 8000i in a DHCP Reply Packet, the hostname is ignored.

An administrator can change the **"hostname"** parameter for the DHCP Option 12 via the configuration files.

To Configure DHCP Option 12 Hostname:

Use the following procedure to configure DHCP Option 12 Hostname on the BluStar 8000i.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [DHCP Option Settings on page A-10](#).

Using Option 77 User Class

DHCP Option 77 User Class is sent in DHCP request packets from the BluStar 8000i to the configuration server. Option 77 defines specific User Class identifiers to convey information about a BluStar 8000i's software configuration or about its user's preferences.

For example, you can use the User Class Option to configure all BluStar 8000is in the Accounting Department with different user preferences than the BluStar 8000is in the Marketing Department. A DHCP server uses the User Class option to choose the address pool for which it allocates an address from, and/or to select any other configuration option.

Notes:

- If the User Class is not specified (left blank) in the DHCP request packet, the BluStar 8000i does not send the User Class DHCP Option 77.
- Multiple User Classes inside a DHCP Option 77 are not supported.
- DHCP Option 77 may affect the precedence of DHCP Options, dependent on the DHCP Server.

An administrator can configure the **"dhcp userclass"** parameter via the configuration files.

To Configure DHCP Option 77 User Class:

Use the following procedure to configure DHCP Option 77 User Class on the BluStar 8000i.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [DHCP Option Settings](#) on page A-10.

Using Options 159 and 160

In addition to DHCP Option 66, the BluStar 8000i also supports DHCP Options 159 and 160. The BluStar 8000i uses the following order of precedence when deriving the configuration server parameters: 43, 160, 159, 66.

An administrator can override this order of precedence by setting the **"dhcp config option override"** parameter. Setting this parameter results in the BluStar 8000i only using the chosen DHCP option and ignoring the other options.

For more information about setting DHCP download preference, see [Configuration Server Download Precedence](#) on page 3-6.

WARNING!

Administrators should review the updated BluStar 8000i DHCP option precedence order and configuration options to avoid potential impact to existing Aastra BluStar 8000i deployments.

To Configure DHCP Download Options on the BluStar 8000i:

Use the following procedure to configure DHCP Option Override on the BluStar 8000i:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [DHCP Option Settings](#) on page A-10.

Configuration Server Download Precedence

An administrator can set the BluStar 8000i's download precedence to ignore DHCP, (**only during the boot when the remote configuration server is contacted**) and use the following precedence instead:

1. DHCP *,
2. Configuration URI, and then,
3. Direct configuration.

* DHCP is first unless it is disabled (override = "-1")

To configure the download precedence, you use the option value "-1" as the value for the "**dhcp config option override**" parameter in the configuration files. Setting this parameter to "-1" causes all DHCP configuration options to be ignored.

To Configure a Download Precedence Using the Configuration Files:

Use the following procedure to configure the DHCP Download Precedence using the configuration files:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [DHCP Option Settings](#) on page A-10.

DNS Caching

The BluStar 8000i has the ability to cache DNS requests according to RFC1035 and RFC2181. The BluStar 8000i caches DNS lookups according to the TTL field, so that it only performs another lookup for an address when the TTL expires.

Configuring Network Settings Manually

If you disable DHCP on your BluStar 8000i, you need to configure the following network settings manually:

- IP Address
- Subnet Mask
- Gateway
- Primary DNS
- Secondary DNS

To Configure a Network Settings Manually:

You can configure the network settings using the configuration files.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Network Settings](#) on page A-4.

Configuring LAN and PC Port Negotiation

Ethernet is the computer networking technology for local area networks (LANs). You use the LAN Port to connect to a LAN using a twisted pair 10BASE-T cable to transmit 10BASE-T Ethernet. You use the PC Port to connect to the configuration server (your PC).

There are two Ethernet ports on the rear of the BluStar 8000i: LAN Port  and PC Port .

The BluStar 8000i supports each of the following methods of transmission:

- Auto-negotiation
- Half-duplex (10Mbps, 100Mbps, or 1000Mbps)
- Full-duplex (10Mbps, 100Mbps, or 1000Mbps)

Auto-negotiation

Auto-negotiation is when two connected devices choose common transmission parameters. In the auto-negotiation process, the connected devices share their speed and duplex capabilities and connect at the highest common denominator (HCD). Auto-negotiation can be used by devices that are capable of different transmission rates (such as 10Mbps/sec, 100Mbps/sec, or 1000Mbps/sec), different duplex modes (half duplex and full duplex) and/or different standards at the same speed. You can set the LAN and PC Ports on the BluStar 8000i to auto-negotiate during transmission.

Half-Duplex (10Mbps, 100Mbps, or 1000Mbps)

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time. For example, on a LAN using a technology that has half-duplex transmission, one device can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Half-duplex transmission implies a bidirectional line (one that can carry data in both directions). On the BluStar 8000i, you can set the half-duplex transmission to transmit in 10Mbps, 100Mbps, or in 1000Mbps.

Full-Duplex (10Mbps, 100Mbps, or 1000Mbps)

Full-duplex data transmission means that data can be transmitted in both directions on a signal carrier at the same time. For example, on a LAN with a technology that has full-duplex transmission, one device can be sending data on the line while another device is receiving data. Full-duplex transmission implies a bidirectional line (one that can move data in both directions). On the BluStar 8000i, you can set the full-duplex transmission to transmit in 10Mbps, 100Mbps, or in 1000Mbps.

To Configure the LAN Port:

You can configure the “**ethernet port 0**” parameter using the configuration files.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Network Settings on page A-4](#).

Network Time Servers

A time server is a computer server that reads the actual time from a reference clock and distributes this information to the clients in a network. The time server may be a local network time server or an internet time server.

The Network Time Protocol (NTP) is the most widely used protocol that distributes and synchronizes time in the network with the time on the time server. You can enable a time server to synchronize time on the BluStar 8000i with the time server you specify. The time server is enabled by default.

An administrator can use the configuration files to enable/disable the time server using the **"time server disabled"** parameter, and specify a time server 1, time server 2, and/or time server 3 using the **"time server1"**, **"time server2"**, and/or **"time server3"** parameters.

To Configure the NTP Servers:

Use the following procedure to enable/disable the time server and optionally set the IP address of time servers 1, 2, and/or 3.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Network Settings](#) on page A-4.

Type of Service (ToS), Quality of Service (QoS), and DiffServ QoS

ToS is an octet as a field in the standard IP header. It is used to classify the traffic of the different QoSs.

QoS provides service differentiation between IP packets in the network. This service differentiation is noticeable during periods of network congestion (for example, in case of contention for resources) and results in different levels of network performance.

Differentiated Service (DiffServ) QoS is class-based where some classes of traffic receive preferential handling over other traffic classes.

The Differentiated Services Code Point (DSCP) value is stored in the first six bits of the ToS field. Each DSCP specifies a particular per-hop behavior that is applied to a packet. DSCP bits in the ToS field of the IP header are set for SIP and RTP (audio and video) packets using either the default values or the values configured via the following parameters.

Parameters in Configuration Files	Description
tos sip	Specifies the Differentiated Services Code Point (DSCP) for SIP packets.
tos rtp	Specifies the Differentiated Services Code Point (DSCP) for audio RTP packets.
tos rtp video	Specifies the Differentiated Services Code Point (DSCP) for video RTP packets.

Note:

ToS/DSCP is enabled by default and the **"tos sip"**, **"tos rtp"**, and **"tos rtp video"** parameters have default values of 46.

To Configure ToS/QoS/DiffServ QoS:

Use the following procedures to configure ToS/QoS/DiffServ QoS.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [ToS/QoS/Diffserv QoS Parameters](#) on page A-8.

Virtual Local Area Network (VLAN)

VLAN is a feature on the BluStar 8000i that allows for multiple logical Ethernet interfaces to send outgoing RTP packets over a single physical Ethernet as described in IEEE Std 802.3. On the terminal, you configure a VLAN ID that associates with the physical Ethernet port 0 (LAN port).

By configuring specific VLAN parameters, the BluStar 8000i has the capability of adding tags and processing the ID and priority information contained within the tag.

VLAN on the BluStar 8000i is disabled by default. When you enable VLAN, the terminal provides defaults for all VLAN parameters. If you choose to change these parameters, you can configure them using the configuration files.

The following parameters allow an administrator to configure the VLAN feature:

Parameters in Configuration Files	Description
Global	
tagging enabled	Enables or disables VLAN on the BluStar 8000i.
LAN Port	
vlan id	Used to configure a VLAN ID that associates with the physical Ethernet Port 0.
qos eth port 0 priority	Specifies the priority value used for all traffic (e.g. SIP, RTP, etc.) on the physical Ethernet Port 0.
PC Port	
vlan id port 1	Specifies the VLAN ID used to pass packets through to a PC via Port 1.
qos eth port 1 priority	Specifies the priority value used for passing VLAN packets through to a PC via Port 1.

Notes:

- In order for the software to successfully maintain connectivity with a network using VLAN functionality, the terminal must be restarted if you modify the "**tagging enabled**", "**vlan id**", or "**vlan id port 1**" parameters.
- Traffic from both Ethernet Port 0 and Ethernet Port 1 must be tagged with the appropriate VLAN IDs. Packets tagged with other VLAN IDs or untagged packets will be discarded by the respective port.

To Configure VLAN:

Note:

VLAN functionality can be enabled/disabled through the BluStar 8000i terminal UI. For more information, see [Terminal Identity](#) on page 4-2.

Use the following procedures to configure the VLAN feature.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Virtual Local Area Network \(VLAN\) Settings](#) on page A-8.

Virtual Private Network (VPN)

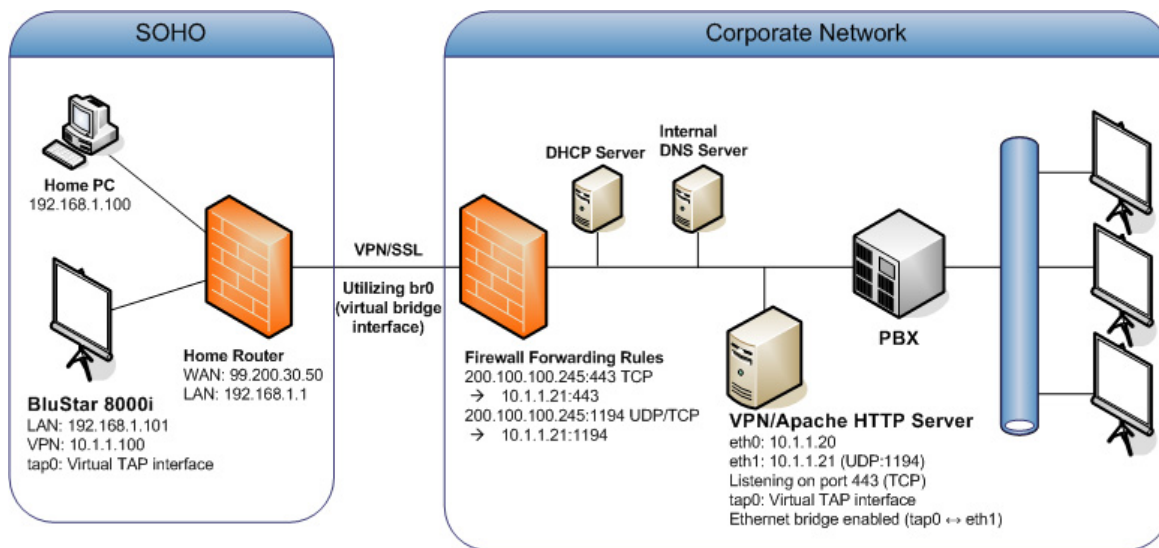
The BluStar 8000i integrates an OpenVPN client for authentication and remote access to the corporate network. OpenVPN is a highly-flexible open-source VPN application available for a multitude of operating systems that utilizes SSL/TLS for key exchange. Utilizing OpenVPN Access Server, administrators can set up and configure their networks to allow remote terminals access to the corporate network ensuring that all the conferencing and collaboration capabilities of the BluStar 8000i can be fully utilized in a remote environment.

Note:

VPN is a licensed feature. See [Licensing](#) on page 4-43 for more information.

Overview

The image below details an overview of how OpenVPN can be implemented in a typical corporate environment.



Server-Side

On the server-side, an ethernet bridge is created with tap0 (i.e. a virtual TAP interface) and eth1 (i.e. the secondary ethernet card). Any broadcasted or received traffic from tap0 is duplicated to eth1 and vice versa.

Client-Side

On the client side, once the connection to the server has been established, the following tunnel is created:

- Client tap0 <br0> Server tap0 <Ethernet Bridge> eth1 <-> Corporate LAN.

The client will send a DHCP request through the tunnel to the DHCP server on the corporate network and the DHCP reply will be sent back to the client allowing for the client to receive an internal IP on tap0.

After the internal IP has been established, the client's BluStar will function through the VPN (i.e. function as a local terminal on the corporate network).

Note:

Once an internal IP is established, the client's default gateway will be switched to the server; therefore all internet traffic from the client will run through the server as well.

Configuring the Network for OpenVPN

Sample configuration files/scripts and a simplified configuration example using Fedora 13 is available in [Appendix C. "OpenVPN Configuration"](#).

SIP Account Settings

Description

The BluStar 8000i uses Session Initiation Protocol (SIP) account information to register with the SIP Call Server. The BluStar 8000i defines network and user account parameters that apply to all lines/call appearances. You configure and modify these parameters and associated values using the configuration files. Basic SIP settings include authentication and network settings. Advanced SIP settings include other features you can configure on the BluStar 8000i.

This section describes the following information:

- [Basic SIP Settings](#)
- [Advanced SIP Settings \(optional\)](#)
- [Real-time Transport Protocol \(RTP\) Settings](#)

Basic SIP Settings

The BluStar 8000i has one SIP account with two lines/call appearances. The following table identifies the SIP authentication and network parameters on the BluStar 8000i.

SIP Authentication Parameters

Parameters in Configuration Files	Description
sip user name	User name used in the name field of the <i>SIP URI</i> for the BluStar 8000i and for registering the BluStar 8000i at the registrar. Valid values are up to 20 alphanumeric characters. For example, sip user name: 1010
sip display name	Used in the display name field of the <i>From</i> SIP header field. Some IP PBX systems use this as the caller's ID and some may overwrite this with the string that is set at the PBX system. Valid values are up to 20 alphanumeric characters. For example, sip display name: Joe Smith
sip screen name	Used to display text on the screen of the BluStar 8000i. You may want to set this parameter to display the user's name on the BluStar 8000i. Valid values are up to 20 alphanumeric characters. For example, sip screen name: Joe Smith
sip screen name 2	Used to display text on a second line on the screen of the BluStar 8000i. Valid values are up to 20 alphanumeric characters. For example, sip screen name 2: Lab Phone
sip auth name	Used in the username field of the Authorization header field of the SIP REGISTER request. Valid values are up to 20 alphanumeric characters. For example, sip auth name: 5553456
sip password	Password used to register the BluStar 8000i with the SIP proxy. Valid values are up to 20 alphanumeric characters. Passwords are encrypted and display as asterisks when entering. For example, sip password: 12345
sip mode	The mode-type that you assign to the BluStar 8000i. Valid values are Generic (0), BroadSoft SCA (1), Reserved for (2), or BLA (3). Default is Generic (0). For example, sip mode: 2

SIP Network Parameters

Parameters in Configuration Files	Description
sip proxy ip	The IP address of the SIP proxy server for which the BluStar 8000i uses to send all SIP requests. A SIP proxy is a server that initiates and forwards requests generated by the BluStar to the targeted user. Up to 64 alphanumeric characters. For example, sip proxy ip: 192.168.0.101
sip proxy port	The proxy server's port number. Default is 0. For example, sip proxy port: 5060
sip outbound proxy	This is the address of the outbound proxy server. All SIP messages originating from the BluStar 8000i are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here. Default is 0.0.0.0. For example, sip outbound proxy: 10.42.23.13
sip outbound proxy port	The proxy port on the proxy server to which the BluStar 8000i sends all SIP messages. Default is 0. For example, sip outbound proxy port: 5060
sip registrar ip	The address of the registrar for which the BluStar 8000i uses to send <i>REGISTER</i> requests. A SIP registrar is a server that maintains the location information of the BluStar 8000i. A value of 0.0.0.0 disables registration. However, the BluStar 8000i is still active and you can dial using the username@ip address of the BluStar 8000i. For example, sip registrar ip: 192.168.0.101
sip registrar port	The registrar's port number. Default is 0. For example, sip registrar port: 5060
sip registration period	The requested registration period, in seconds, from the registrar. For example, sip registration period: 3600

To Configure SIP Settings:

Use the following procedure to configure the SIP Authentication and Network Settings on the BluStar 8000i.

**Configuration Files**

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [SIP Settings](#) on page A-20.

Advanced SIP Settings (optional)

Advanced SIP Settings on the BluStar 8000i allow you to configure specific features. The following list provides Advanced SIP Settings that you can configure using the configuration files.

SIP Advanced Settings

Parameters in Configuration Files	Description
sip explicit mwi subscription	If the BluStar 8000i has a message waiting subscription with the service provider, a message waiting indicator (MWI) (LED or display icon) tells the user there is a message on the BluStar 8000i. This parameter is disabled by default. For example, sip explicit mwi subscription: 1
sip explicit mwi subscription period	The requested duration, in seconds, before the MWI subscription times out. The BluStar 8000i re-subscribes to MWI before the subscription period ends. Default value is 86400. For example, sip explicit mwi subscription period: 30
sip out-of-band dtmf	The BluStar 8000i supports out-of-band Dual-Tone Multi-frequency (DTMF) mode according to RFC2833. The "out-of-band dtmf" parameter is enabled by default. In out-of-band mode, the DTMF audio is automatically clamped (muted) and DTMF digits are not sent in the RTP packets. For example, sip out-of-band dtmf: 0
sip dtmf method	Sets the dual-tone multifrequency (DTMF) method used on the BluStar 8000i to send DTMF digits from the BluStar 8000i via INFO messages. You can set the DTMF method as RTP, SIP info, or both. Default is 0 (RTP). For example, sip dtmf method: 1
sip send mac	Adds an "Aastra-Mac:" header to the SIP REGISTER messages sent from the BluStar 8000i to the call server, where the value is the MAC address of the BluStar 8000i. For example, sip send mac: 1 For more information, see MAC Address in REGISTER Messages on page 5-2 .
sip session timer	The time, in seconds, that the BluStar 8000i uses to send periodic re-INVITE requests to keep a session alive. The proxy uses these re-INVITE requests to maintain the status of the connected sessions. See RFC4028 for details. Default is 0. For example, sip session timer: 30
sip T1 timer sip T2 timer	These timers are SIP transaction layer timers defined in RFC 3261. Timer 1 is an estimate, in milliseconds, of the round-trip time (RTT). Timer 2 represents the amount of time, in milliseconds, a non-INVITE server transaction takes to respond to a request. For example, sip T1 timer: 600 For example, sip T2 timer: 8
sip transaction timer	The amount of time, in milliseconds that the BluStar 8000i allows the callserver (registrar/proxy) to respond to SIP messages that it sends. If the BluStar 8000i does not receive a response in the amount of time designated for this parameter, the BluStar 8000i assumes the message has timed out. For example, sip transaction timer: 6000
sip blacklist duration	Specifies the length of time, in seconds, that a failed server remains on the server blacklist. The BluStar 8000i avoids sending a SIP message to a failed server (if another server is available) for this amount of time. For example, sip blacklist duration: 600
sip whitelist	This parameter enables/disables the whitelist proxy feature, as follows: <ul style="list-style-type: none"> Set to 0 to disable the feature. Set to 1 to enable the feature. When this feature is enabled, a BluStar 8000i accepts call requests from a trusted proxy server <i>only</i>. The BluStar 8000i rejects any call requests from an untrusted proxy server. For example, sip whitelist: 1
sip xml notify event	Enables or disables the BluStar 8000i to accept or reject an aastra-xml SIP NOTIFY message. For example, sip xml notify event: 1 Note: To ensure that the SIP NOTIFY message is coming from a trusted source, it is recommended that you enable the Whitelist feature (Whitelist Proxy parameter) on the BluStar 8000i. If enabled, and the BluStar 8000i receives a SIP NOTIFY from a server that is NOT on the whitelist (i.e. untrusted server), the BluStar 8000i rejects the message.

To Configure Advanced SIP Settings

Use the following procedures to configure the Advanced SIP Settings on the BluStar 8000i.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Advanced SIP Settings](#) on [page A-25](#).

Real-time Transport Protocol (RTP) Settings

Real-time Transport Protocol (RTP) is used as the bearer path for voice packets sent over the IP network. Information in the RTP header tells the receiver how to reconstruct the data and describes how the bit streams are packetized (i.e. which codec is in use). Real-time Transport Control Protocol (RTCP) allows endpoints to monitor packet delivery, detect and compensate for any packet loss in the network. SIP and H.323 both use RTP and RTCP for the media stream, with User Datagram Protocol (UDP) as the transport layer encapsulation protocol.

You can set the following parameters for RTP on the BluStar 8000i:

- sip out-of-band dtmf
- sip dtmf method

Out-of-Band DTMF

The BluStar 8000i supports out-of-band Dual-Tone Multifrequency (DTMF) mode according to RFC2833. The "**out-of-band DTMF**" parameter is enabled by default. In out-of-band mode, the DTMF audio is automatically clamped (muted) and DTMF digits are not sent in the RTP packets.

DTMF Method

Sets the dual-tone multifrequency (DTMF) method used on the BluStar 8000i to send DTMF digits from the BluStar 8000i via INFO messages. You can set the DTMF method as RTP, SIP info, or both. Default is 0 (RTP).

Configuring RTP Features

Use the following procedures to configure the RTP settings on the BluStar 8000i.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Advanced SIP Settings](#) on [page A-25](#).

Chapter 4

Configuring Operational Features

The BluStar 8000i has specific operational features that you can configure. This chapter describes each feature and provides procedures for configuring a BluStar 8000i to use the following features:

- [Terminal Identity](#)
- [Factory Defaults](#)
- [Power Saving Schedule](#)
- [User Settings](#)
- [Terminal Security Settings](#)
- [Screen Settings](#)
- [Locale Settings](#)
- [Audio/Video Settings](#)
- [Call Forward Settings](#)
- [Incoming Intercom Call Auto-Answer Settings](#)
- [History](#)
- [Directory](#)
- [Basic LDAP Settings](#)
- [Advanced LDAP Settings \(optional\)](#)
- [Microsoft Exchange Contacts](#)
- [LDAP Directory/Exchange Contacts Update Interval](#)
- [Voicemail](#)
- [Video Voicemail Client Integration](#)
- [Emergency Dial Plan](#)
- [Busy Lamp Field \(BLF\)](#)
- [BLF Subscription Period](#)
- [Directed Call Pickup](#)
- [Diversion Display](#)
- [Shared Call Appearance \(SCA\) and SCA Call Bridging](#)
- [XML Settings](#)
- [Licensing](#)

BluStar 8000i Settings

Terminal Identity

In the **tools** menu on the BluStar 8000i UI, you can specify the **terminal identity** connection settings used by the terminal to communicate with your network.

The screenshot shows the BluStar 8000i settings interface with the 'terminal identity' tab selected. The interface is divided into two main sections: 'network settings' and 'identity'. The 'network settings' section includes fields for MAC address (70:71:BC:88:0D:DA), use DHCP (checked), IP address (10.30.102.122), net mask (255.255.255.0), default gateway (10.30.102.1), primary DNS (10.30.2.34), and secondary DNS (10.30.2.46). The 'identity' section includes a terminal name field (BluStar) and an 'advanced' button.

When a user is logged off of a BluStar 8000i, you can enter information in the following fields on the main terminal identity screen:

Field	Description
Network Settings	
use DHCP	The BluStar 8000i is capable of querying a DHCP server. If DHCP is disabled, manually enter the configuration server's IP address. For more information, see DHCP on page 3-3 .
IP address	IP address of the BluStar 8000i. To assign a static IP address, disable DHCP. For more information, see Configuring Network Settings Manually on page 3-6 .
net mask	Subnet mask defines the IP address range local to the BluStar 8000i. To assign a static subnet mask, disable DHCP. For more information, see Configuring Network Settings Manually on page 3-6 .
default gateway	The IP address of the network's gateway or default router IP address. To assign a static Gateway IP address, disable DHCP. For more information, see Configuring Network Settings Manually on page 3-6 .
primary DNS	Primary domain name server IP address. For any of the IP address settings on the BluStar 8000i a domain name value can be entered instead of an IP address. With the help of the domain name servers, the domain names for such parameters can then be resolved to their corresponding IP addresses. To assign static DNS addresses, disable DHCP. If a host name is configured on the BluStar 8000i, you must also set a DNS. For more information, see Configuring Network Settings Manually on page 3-6 .
secondary DNS	A service that translates domain names into IP addresses. To assign static DNS addresses, disable DHCP. For more information, see Configuring Network Settings Manually on page 3-6 .

Field	Description
Identity	
terminal name	NA in SIP Call Server mode.

Touching the **advanced** button displays the advanced terminal identity options.

The advanced terminal identity screen allows you to configure the following settings:

Field	Description
Call Server	
server type	Specifies if the BluStar 8000i is in BluStar Application Server mode or SIP Call Server mode.
configuration server	Specifies the BluStar 8000i's configuration server's IP address. For more information, see Configuration Server Settings on page 2-10 .
VPN	
use VPN	Enables the client-side Virtual Private Network (VPN) connection for remote access to the SIP Call Server network.
certificate location	Specifies the VPN certificate location. For more information, see Virtual Private Network (VPN) on page 3-10 .
Network Settings	
use IPv6	Enables IP version 6 that will depreciate IP version 4.
disable autonegotiate	Auto-negotiate is when two connected devices choose common transmission parameters. By default, the BluStar 8000i will auto-negotiate during transmission. In the auto-negotiation process, the connected devices share their speed and duplex capabilities and connect at the highest common denominator (HCD). Auto-negotiation can be used by devices that are capable of different transmission rates (such as 10Mbps/sec, 100Mbps/sec, or 1000Mbps/sec), different duplex modes (half duplex and full duplex), and/or different standards at the same speed. You can disable autonegotiate on the BluStar 8000i. For more information, see Configuring LAN and PC Port Negotiation on page 3-7 .
MTU	Displays the maximum size of packet you can send. If a packet is larger than 1500 it will send multiple packets up to 1500 each in size.

Field	Description
VLAN	
use VLAN	Enables the Virtual Local Area Network (VLAN) feature. For more information, see Virtual Local Area Network (VLAN) on page 3-9 .
VLAN id	Specifies the VLAN ID that associates with the physical Ethernet Port 0. For more information, see Virtual Local Area Network (VLAN) on page 3-9 .

Factory Defaults

You can set the BluStar 8000i to its factory default setting on the BluStar 8000i UI. Factory default settings are the settings that reside on the BluStar 8000i after it has left the factory. Factory default settings on the BluStar 8000i set factory defaults for all of the settings in the `aastra.cfg`, `<model>.cfg`, and `<mac>.cfg` files.

Note:

Resetting the terminal to factory default will not change the `<user>.cfg`.

To Reset to Factory Defaults:

1. Touch the **app menu** button.
2. Touch **tools >utilities**.
3. Touch the **reset to factory defaults** button.
The following message appears: *"Do you really want to log off and reset to factory defaults?"*
4. Press either **Reset** or **Cancel**.

Power Saving Schedule

The BluStar 8000i integrates a power saving Eco-Off mode. Administrators can enable Eco-Off mode by defining the BluStar 8000i user's normal operating work schedule. During the period of time outside of the specified work schedule, the BluStar 8000i will automatically power down all extraneous hardware components and a screen saver will be initialized, thereby allowing for a reduction in overall energy consumption and in turn a decrease in operating costs. Users can "wake up" the BluStar 8000i while in Eco-Off mode by either touching the screen, pressing any hard key, or lifting the handset.

Notes:

- If the BluStar 8000i is "woken up" while in Eco-Off mode, the BluStar 8000i will not return to Eco-Off mode until the next scheduled power saving period.
- If the BluStar 8000i is in an active call or in use at the time Eco-Off mode is set to initialize, Eco-Off mode will be delayed until the BluStar 8000i is idle.
- All incoming calls will be ignored by the BluStar 8000i if it is in Eco-Off mode (i.e. a 480 Temporarily Unavailable response will be sent to the caller's device).

power saving schedule

please select normal operating/business hours
(8000i will be in eco-off mode outside of this schedule)

work days

sun mon tue wed thu fri sat all

☐ ☒ ☒ ☒ ☒ ☒ ☐ ☐

work hours

start end

weekdays 09 : 00 AM 05 : 00 PM

weekend HH : MM AM HH : MM AM same as weekdays ☒

The power saving schedule can be configured directly on the BluStar 8000i by navigating to the Power Saving Schedule screen in the Utilities menu of the Tools application. Administrators have the additional option of configuring the power saving schedule by defining the following parameters in the configuration files:

Notes:

- The value ranges for the “working hour [weekday/weekend] [start/end]” parameters are dependent on the time format of the respective BluStar 8000i (i.e. 12-hour or 24-hour).
- If the BluStar 8000i is set to the 24-hour format, the “working pm [weekday/weekend] [start/end]” parameters should not be defined in the configuration files.
- The term “weekday” for the Power Saving Schedule feature on the BluStar 8000i refers to the days from Monday to Friday. The term “weekend” refers to Saturday and Sunday.

Parameter in Configuration Files	Description
user defined power savings schedule	Specifies whether or not users are allowed to configure the power saving schedule on their BluStar 8000i. If enabled, users will be allowed to configure their own power saving schedule. Example: user defined power savings schedule: 0
working monday	Specifies whether or not Mondays are part of the BluStar 8000i user's normal work week. Example: working monday: 1
working tuesday	Specifies whether or not Tuesdays are part of the BluStar 8000i user's normal work week. Example: working tuesday: 1
working wednesday	Specifies whether or not Wednesdays are part of the BluStar 8000i user's normal work week. Example: working wednesday: 1
working thursday	Specifies whether or not Thursdays are part of the BluStar 8000i user's normal work week. Example: working thursday: 1
working friday	Specifies whether or not Fridays are part of the BluStar 8000i user's normal work week. Example: working friday: 1
working saturday	Specifies whether or not Saturdays are part of the BluStar 8000i user's normal work week. Example: working saturday: 0
working sunday	Specifies whether or not Sundays are part of the BluStar 8000i user's normal work week. Example: working sunday: 0
working all days	Specifies whether or not the BluStar 8000i user's normal work week consists of all they days of the week. Example: working all days: 0
working hour weekday start	Specifies the starting hour of the BluStar 8000i user's weekday work schedule. Example: working hour weekday start: 9 Notes: <ul style="list-style-type: none"> • Ranges for this parameter are dependent on the time format of the respective BluStar 8000i. • The term “weekday” refers to the days from Monday to Friday.

Parameter in Configuration Files	Description
working minute weekday start	<p>Specifies the starting minute of the BluStar 8000i user's weekday work schedule. Example: working minute weekday start: 15</p> <p>Note: The term "weekday" refers to the days from Monday to Friday.</p>
working pm weekday start	<p>Specifies whether the BluStar 8000i user's weekday work schedule start time defined in the "working hour weekday start" and "working minute weekday start" parameters is AM or PM. Example: working pm weekday start: 0</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter should only be used if the BluStar 8000i is using the 12-hour time format. The term "weekday" refers to the days from Monday to Friday.
working hour weekday end	<p>Specifies the ending hour of the BluStar 8000i user's weekday work schedule. Example: working hour weekday end: 5</p> <p>Notes:</p> <ul style="list-style-type: none"> Ranges for this parameter are dependent on the time format of the respective BluStar 8000i. The term "weekday" refers to the days from Monday to Friday.
working minute weekday end	<p>Specifies the ending minute of the BluStar 8000i user's weekday work schedule. Example: working minute weekday end: 30</p> <p>Note: The term "weekday" refers to the days from Monday to Friday.</p>
working pm weekday end	<p>Specifies whether the BluStar 8000i user's weekday work schedule end time defined in the "working hour weekday end" and "working minute weekday end" parameters is AM or PM. Example: working pm weekday end: 1</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter should only be used if the BluStar 8000i is using the 12-hour time format. The term "weekday" refers to the days from Monday to Friday.
working hour weekend start	<p>Specifies the starting hour of the BluStar 8000i user's weekend work schedule. Example: working hour weekend start: 11</p> <p>Notes:</p> <ul style="list-style-type: none"> Ranges for this parameter are dependent on the time format of the respective BluStar 8000i. The term "weekend" refers to Saturday and Sunday.
working minute weekend start	<p>Specifies the starting minute of the BluStar 8000i user's weekend work schedule. Example: working minute weekend start: 30</p> <p>Note: The term "weekend" refers to Saturday and Sunday.</p>
working pm weekend start	<p>Specifies whether the BluStar 8000i user's weekend work schedule start time defined in the "working hour weekend start" and "working minute weekend start" parameters is AM or PM. Example: working pm weekend start: 0</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter should only be used if the BluStar 8000i is using the 12-hour time format. The term "weekend" refers to Saturday and Sunday.
working hour weekend end	<p>Specifies the ending hour of the BluStar 8000i user's weekend work schedule. Example: working hour weekend end: 3</p> <p>Notes:</p> <ul style="list-style-type: none"> Ranges for this parameter are dependent on the time format of the respective BluStar 8000i. The term "weekend" refers to Saturday and Sunday.
working minute weekend end	<p>Specifies the ending minute of the BluStar 8000i user's weekend work schedule. Example: working minute weekend end: 30</p> <p>Note: The term "weekend" refers to Saturday and Sunday.</p>

Parameter in Configuration Files	Description
working pm weekend end	<p>Specifies whether the BluStar 8000i user's weekend work schedule end time defined in the "working hour week-end end" and "working minute weekend end" parameters is AM or PM. Example: working pm weekend end: 1</p> <p>Notes:</p> <ul style="list-style-type: none"> • This parameter should only be used if the BluStar 8000i is using the 12-hour time format. • The term "weekend" refers to Saturday and Sunday.
weekend working same as weekdays	<p>Specifies whether or not the BluStar 8000i user's weekend work schedule is the same as his/her weekday work schedule. Example: weekend working same as weekdays: 0</p> <p>Note: The term "weekday" for the Power Saving Schedule feature on the BluStar 8000i refers to the days from Monday to Friday. The term "weekend" refers to Saturday and Sunday.</p>

To Configure the Power Saving Schedule Using the Configuration Files:

Use the following procedure to configure the power saving schedule:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Power Saving Schedule Settings on page A-49](#).

To Configure the Power Saving Schedule on the BluStar 8000i UI:

1. Touch the **app menu** button.
2. Touch **tools > utilities**.
3. Touch the **power saving schedule** button.
4. Under **work days**, touch the buttons corresponding to the days of the week that you are normally at work.
or
Touch the **all** button if your normal work week consists of all the days of the week.
5. Under **work hours**, enter the **start** and **end** time of your weekday work schedule by touching the hour (HH) and minute (MM) fields and using the on-screen keyboard. If your terminal is in 12-hour mode, touch the **AM/PM** button to toggle between the two options.
6. Enter the **start** and **end** time of your weekend work schedule by touching the hour (HH) and minute (MM) fields and using the on-screen keyboard. If your terminal is in 12-hour mode, touch the **AM/PM** button to toggle between the two options.
or
Touch the **same as weekdays** button if your weekend work schedule is the same as your weekday work schedule.

Note:

The term "weekday" for the Power Saving Schedule feature on the BluStar 8000i refers to the days from Monday to Friday. The term "weekend" refers to Saturday and Sunday.

7. If you do not have to configure anything else on the screen, touch **done**.

User Settings

User Config File Upload

You can specify the number of seconds until user settings or contacts will be re-uploaded to the server IF there has been a change using the BluStar 8000i **"user config upload"** parameter.

Name and Passwords

The user name and password to retrieve the <user>.cfg and directory files (global.csv and <user>.csv) are configured on the configuration server. The SIP user name and password are configured on the SIP Call Server that the BluStar 8000i will login to.

Terminal Security Settings

Administrators can set terminal security settings using the parameters listed below.

Require Settings Password

You can specify if a password should be required to edit the BluStar 8000i terminal identity using the **"require settings password"** parameter.

Settings Password

If the **"require settings password"** parameter is enabled, you can specify the required password by using the **"settings password"** parameter.

Disable Dialing When Logged Off

You can disable dialing when no user is logged into the BluStar 8000i terminal using the **"logoff disable dial"** parameter. Disabling dialing will cause the terminal to not display the dial pad.

Auto Answer


You can specify whether or not to allow users to change auto answer settings by using the **"auto answer"** configuration parameter. Additionally, this parameter must be enabled for the **"sip allow auto answer"** parameter (i.e. to enable/disable auto-answering of incoming intercom calls) to have any effect (see [Incoming Intercom Call Auto-Answer Settings](#) on [page 4-13](#)).

To Configure Auto Answer on the BluStar 8000i UI:

1. Touch the **app menu** button.
2. Touch **tools > call handling**.
3. Touch the **auto answer** button.
4. Select either:
 - instantly
 - after x rings (i.e. x = 1-10 rings)

Notes:

- If you select "off" you will not be able to configure auto answer for "if in call or conference".
 - The option "If in call with non BluStar device" is not available in SIP Call Server mode.
 - If the **"sip allow auto answer"** parameter is enabled, incoming intercom calls will always be answered instantly even if the auto answer setting is configured for "after x rings".
5. Touch the **if in call or conference** button.

6. Select either:
 - **decline new call and remain in old call**
 - **conference new call into old call**
 - **answer new call and disconnect old call**
 - **answer new call and put old call on hold**
7. If you don't have to configure anything else on the screen, touch **done**. When auto answer is configured, you will see a  symbol on the top of the Home screen.

Force Reboot Time

You can reboot a BluStar 8000i at a specified time using the “**auto reboot**” parameter. The format for this parameter is **yyyy-mm-dd hh:mm:ss** (for ASAP use current date and time).

Screen Lock With Inactivity

You can set the screen to lock after a specified period of inactivity using the “**screen lock time**” parameter. Once a BluStar 8000i is locked, the system requires the currently logged in user's password to be re-entered before the terminal can be used again. Administrators and users can also manually lock/unlock a BluStar 8000i using the BluStar UI (see [Lock Screen](#) on [page 1-23](#)).

To Configure Terminal Security Settings:

Use the following procedure to configure terminal security settings:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Terminal Security Settings](#) on [page A-56](#).

Screen Settings

Administrators can modify the screen dimming and screen saver settings using the parameters listed below.

Screen Dimming

The screen first dim time can be disabled or set to a specified number of seconds, minutes, hours, or days (ranging from 1-10000) using the **"screen 1st dim time"** parameter. The screen partially dims after this set value.

The screen second dim time can be disabled or set to a specified number of seconds, minutes, hours, or days (ranging from 1-10000) using the **"screen 2nd dim time"** parameter. The screen further dims after this set value.

Screen Saver

The screen saver time can be disabled or set to a specified number of seconds, minutes, hours, or days (ranging from 1-10000) using the **"screen save time"** parameter.

Show Cursor

You can configure if the mouse cursor will display on the BluStar 8000i using the **"show cursor"** parameter.

To Configure Screen Settings:

Use the following procedure to configure screen settings:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Screen Settings](#) on page A-58.

Locale Settings

The BluStar 8000i supports several different languages, time zones, and date and time formats. When you specify the language to use, all of the screens display in that language. Administrators can modify the language, time zone, and date and time format settings using the parameters listed below.

Language

You can specify the language to be used on the BluStar 8000i UI using the **"language name"** parameter. The BluStar 8000i UI is available in the following languages:

- English (default)
- French
- German
- Italian
- Japanese
- Simplified Chinese
- Spanish

Time Zone

You can specify the time zone using the **"time zone name"** parameter. The default time zone is "us-eastern".

Date and Time Format

You can specify the date and time formats using the **"date format"** and **"time format"** parameters. The default date format is "WWW MMM DD", while the default time format is the 12 hr format.

Notes:

- These parameters affect how the date and time are displayed on the home screen, in all the applications, and in the call logs.
- If a date format is selected that contains the year, the home screen will not display the year due to space limitations.

To Configure Locale Settings:

Use the following procedure to configure locale settings:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Locale Settings](#) on page A-60.

Audio/Video Settings

Administrators can configure various audio and video settings using the parameters listed below.

Maximum Video Bandwidth Limit

You can set the maximum video bandwidth limit using the **"video max kbitrate"** parameter. This parameter limits the video bandwidth for the terminal to the selected value (either 5000, 3000, 2500, 1500, 768, 384, or 128 kilobits per second).

Maximum Audio Bandwidth Limit

You can set the maximum audio bandwidth limit using the **"audio max kbitrate"** parameter. This parameter limits the audio bandwidth limit for the terminal to the selected value (either 64, 32, 24, or 16 kilobits per second).

Maximum Video Data Transmit and Receive Rates for BluStar 8000i and Non-BluStar 8000i Devices

Asymmetric video data rate support is available allowing administrators and users the ability to independently configure the maximum video data transmit and receive rates for BluStar 8000i and non-BluStar 8000i devices. You can set the maximum data transmit and receive rates using the **"max 8000i h.264 tx rate"**, **"max 8000i h.264 rx rate"**, **"max h.264 tx rate"**, and **"max h.264 rx rate"** parameters. You can also enable or disable the ability to configure these settings in the BluStar 8000i UI (**tools** menu > **call handling** screen) by utilizing the **"user defined video rate"** parameter.

To Configure Audio/Video Settings:

Use the following procedure to configure audio and video settings:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Audio/Video Settings](#) on page A-63.

Call Forward Settings

Call forward (CFWD) allows incoming calls to be forwarded to another destination. The BluStar 8000i sends the SIP message to the SIP proxy, which then forwards the call to the assigned destination. An administrator can configure the “**call forward disabled**” parameter to either enable or disable the ability to configure CFWD on the BluStar 8000i UI. If this parameter is set to “0”, a user and administrator can configure CFWD on the BluStar 8000i UI (**tools** menu > **call handling** screen). If this parameter is set to “1”, all CFWD options are removed from the BluStar 8000i UI, preventing the ability to configure CFWD.

To Enable or Disable Call Forwarding:

Use the following procedure to configure call forwarding:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Call Forward Settings on page A-65](#).

Users can configure call forward settings on their BluStar 8000i UI. Administrators can also configure call forwarding settings in the <user>.cfg file using the following parameters:

- sip forward all state
- sip forward all number
- sip forward busy state
- sip forward busy number
- sip forward no answer state
- sip forward no answer number
- sip ring number

To Configure Call Forward Settings Using the Configuration Files:


Use the following procedure to configure call forwarding:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Call Forward Settings on page A-65](#).

To Configure Call Forward Settings on the BluStar 8000i UI:

1. Touch the **tools** app then **call handling**.
2. Under call forward, touch the **no answer** field to enter in the forwarding number using the on-screen keyboard.
3. Touch the **After 1 ring** button to select how many rings you want to wait until the BluStar 8000i forwards the call.
4. Touch the **all** field to enter in the forwarding SIP URL or number using the on-screen keyboard.
5. Touch the **busy** field to enter in the forwarding SIP URL or number using the on-screen keyboard.
6. If you do not have to configure anything else on the screen, touch **done**.
7. In the telephone feature controls, touch the **forward** button.
The button is outlined in green, indicating call forward is ON. Additionally, you will see a  symbol on the top of the Home screen.

Incoming Intercom Call Auto-Answer Settings

The intercom auto-answer feature allows you to enable or disable automatic answering for an intercom call. In conjunction with the general “**auto answer**” parameter enabled (see [Auto Answer](#) on [page 4-8](#)), when the new “**sip allow auto answer**” parameter is enabled as well, the BluStar 8000i terminal will recognize an incoming intercom call by the information relayed in the “Call-Info” header of the SIP INVITE. It will then place any active calls/conferences on hold and automatically/instantly answer the intercom call.

The BluStar 8000i recognizes if an incoming call is an intercom auto-answer call if the call’s SIP INVITE includes a “Call-Info” header containing “answer-after=0” (e.g. Call-Info: <URI>;answer-after=0).

Notes:

- Both the “**auto answer**” and “**sip allow auto answer**” parameters must be enabled to use the incoming intercom call auto-answer feature.
- Users can change the intercom call auto-answer behavior when in active calls/conferences by configuring auto-answer call handling settings on their BluStar 8000i (see [To Configure Auto Answer on the BluStar 8000i UI](#) on [page 4-8](#)).

To Configure the Incoming Intercom Call Auto-Answer Feature Using the Configuration Files:

Use the following procedure to configure the incoming intercom call auto-answer feature:



Configuration Files

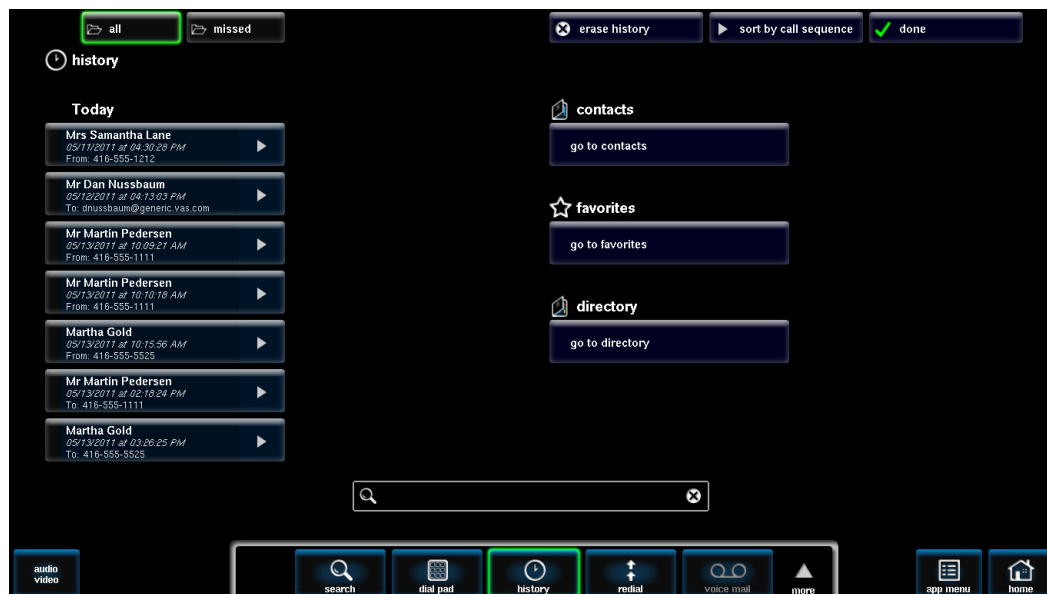
For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Incoming Intercom Call Auto-Answer Settings](#) on [page A-68](#).

History

The history screen displays information about each call that you have either received, missed, or dialed. The BluStar 8000i logs the name and number of the caller, and the date and time of the call. Call history is divided into two folders at the top of the screen: **all** (calls) and **missed** (calls). All calls includes calls that are received and dialed. By default, the contacts in the **all** (calls) or **missed** (calls) folders are sorted by date. You can also sort the contacts by the following:

- first name
- last name
- company then first name
- company then last name
- number or SIP URL
- call sequence

Users can also type in the name of the contact in the search text field, call a contact from this screen, and erase contacts from their call history.



You can enable and disable the history feature using the configuration files. When disabled, the History button will be greyed out and there is no missed calls indicator. When enabled, you can view, scroll, and delete contacts. You can also retrieve missed calls.

To Sort Contacts:

1. Touch the **history** button.
2. Touch the arrow on the **sort by default** button at the top of the screen.
3. Select either:
 - **sort by default**
 - **sort by first name**
 - **sort by last name**
 - **sort by company then first name**
 - **sort by company then last name**
 - **sort by number of SIP URL**
 - **sort by call sequence**

To Erase Call History:

1. Touch the **history** button.
2. Touch the **erase history** button.
The following message appears: *Are you sure you want to erase all call history entries?*
3. Touch **erase call history** or **cancel**.

Enabling/Disabling Call History

You can enable and disable user access to the call history on the BluStar 8000i using the “**callers list disabled**” parameter in the configuration files.

Valid values for this parameter are ‘0’ (enabled) and ‘1’ (disabled). If this parameter is set to ‘0’, the call history can be accessed by all users. If this parameter is set to ‘1’, the BluStar 8000i does not save any caller information to the call history.

Use the following procedure to enable/disable the call history on the BluStar 8000i.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Call History Settings](#) on page A-30.

Missed Calls Indicator

The history button will show a missed calls indicator that increments the number of missed calls. Once a user touches the history button to view the missed calls, the missed calls indicator will disappear from the button.



You can enable and disable the missed calls indicator feature using the configuration files. When disabled, the missed calls indicator does not increment as calls come into the BluStar 8000i.

When enabled, the number of calls that have not been answered increment on the history button. As the number of unanswered calls increment, the phone numbers associated with the calls are stored in the call history. The user can access the call history and clear the calls from the list. Once the user accesses the history screen, the missed calls indicator on the history button is cleared.

Note:

You must have the call history button enabled in order to view the missed calls indicator.

To Retrieve Missed Calls:

1. Touch the **history** button.
2. Select the **missed** folder.
3. Touch a contact button to call them.
OR
Touch the arrow on a contact button.
4. Touch + **add to contacts** or **add to favorites**.
5. Touch the **history** button again to de-select it and close the search screen.

Enabling/Disabling Missed Calls Indicator

You can enable (turn on) and disable (turn off) the missed calls indicator on the BluStar 8000i using the “**missed calls indicator disabled**” parameter in the configuration files. Valid values for this parameter are ‘0’ (enabled) and ‘1’ (disabled). If this parameter is set to ‘0’, the indicator increments as unanswered calls come into the BluStar 8000i. If set to ‘1’, the indicator does not increment the unanswered calls.

Use the following procedure to enable/disable the missed calls indicator on the BluStar 8000i.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Call History Settings](#) on page A-30.

Directory

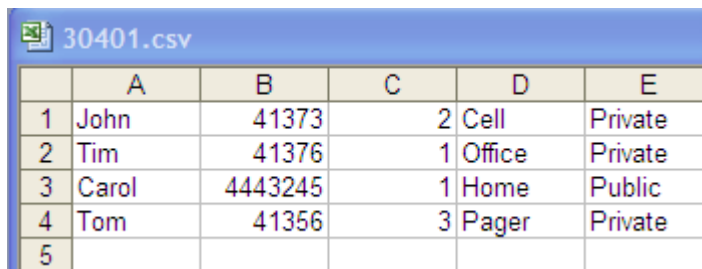
The BluStar 8000i has a directory feature that allows you to store two directories (global and user) in the <user>.cfg file. The **global directory** will populate the directory on the BluStar 8000i UI. The **user directory** will populate the user's contacts (address book). Administrators can also configure LDAP directories that will appear on the users BluStar 8000i directory screen (see [Basic LDAP Settings](#) on [page 4-24](#)).

Notes:

- If enabled, users can choose to have the global directory and the LDAP directory on their BluStar 8000i on the directory screen, or if they select "only use LDAP directory" on the LDAP directory screen, they won't be able to access the global directory set up by the system administrator (see [User Defined LDAP](#) on [page 4-25](#) for more information).
- Users can also add their Microsoft Exchange contacts to their BluStar 8000i address book. If users import their Microsoft Exchange contacts, they will not have access to the user directory (see [Basic LDAP Settings](#) on [page 4-24](#) for more information).

You can perform the following pertaining to the directory:

- You can enable and disable access to the directory list using the <user>.cfg file. When disabled, the directory list does not display on the BluStar 8000i UI, and the **go to directory** button on the UI will be red.
- If the directory list is enabled, you can view, add, change, and delete entries to/from the directory using the BluStar 8000i UI. You can also directly dial a number from the directory.
- You can download the directory list to your PC. The BluStar 8000i stores the *directorylist.csv* file to your PC in comma-separated value (CSV) format.
- You can use any spreadsheet application to open the file for viewing. The following is an example of a directory list in a spreadsheet application.



	A	B	C	D	E
1	John	41373	2	Cell	Private
2	Tim	41376	1	Office	Private
3	Carol	4443245	1	Home	Public
4	Tom	41356	3	Pager	Private
5					

The file displays the name, phone number(s), and line number(s) for each directory entry.

Configuring the Directory List

You can configure the global directory list on the BluStar 8000i using the "**directory 1**" parameter, and the user directory using the "**directory 2**" parameter. You can use these parameters in the following ways:

- to download no directory
- to download a directory from the original configuration server
- to download a directory from another specified server

To download a specific file, the string value must have a filename at the end of the string. For example, directory 1: `ftp://10.30.102.158/path/user.csv`

To Configure the Global and User Directories:

Use the following procedure to configure global and user directories:



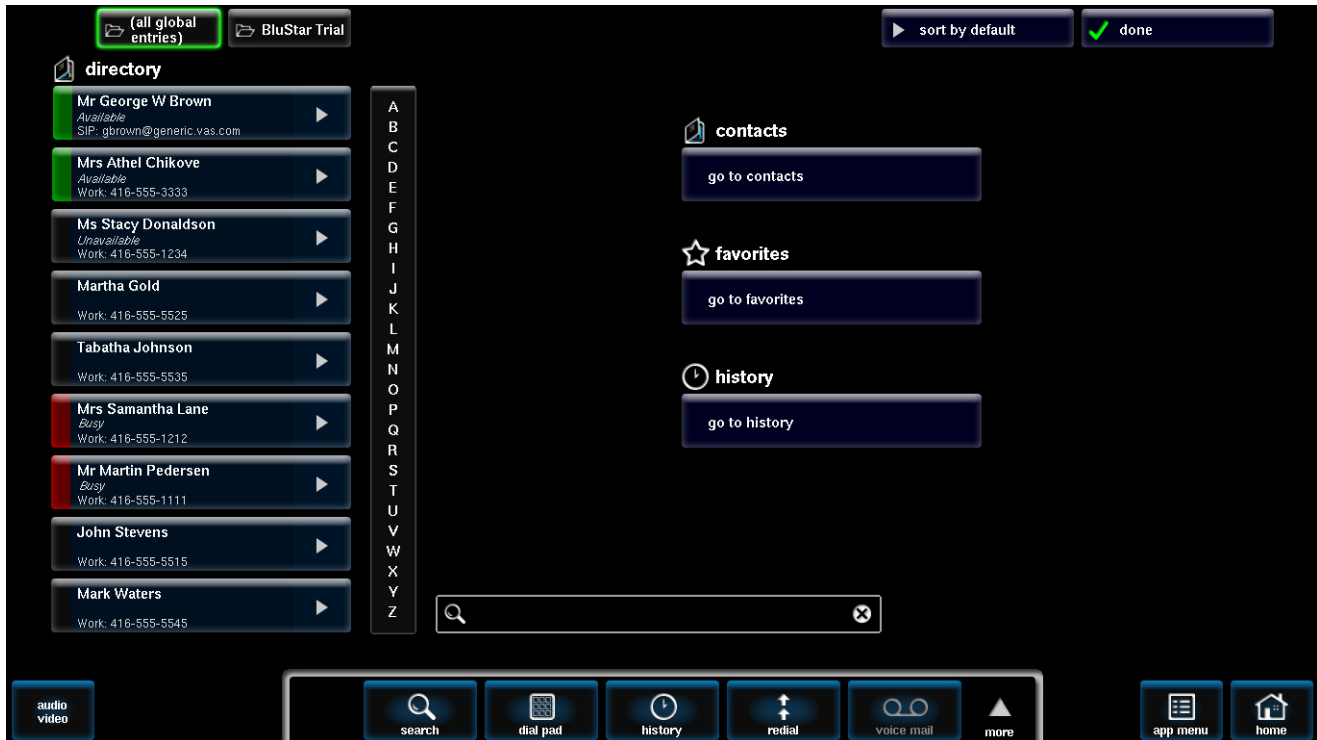
Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Directory Settings](#) on [page A-28](#).

Using the Directory on the BluStar 8000i UI

On the directory screen, you will see all global entries, LDAP directories, and links to your contacts, favorites (including monitored contacts on your BLF list), and call history. When the directory is sorted by default or by first or last name, you can scroll through contacts using a A-Z menu. Contacts can also be sorted by the following:

- default (alphabetic order)
- first name
- last name
- company then first name
- company then last name
- number or SIP URL



Users can also type in the name of the contact they are looking for in the search text field.

To Open the Directory:

1. In the telephone feature controls, touch the **directory** button.
The button is outlined in green, indicating that the directory is open.

To Close the Directory:

1. In the telephone feature controls, touch the **directory** button to de-select it.
OR
On the directory screen, touch **done**.
The button is not outlined in green, indicating that the directory is closed.

To Sort the Directory:

1. In the telephone feature controls, touch the **directory** button.
2. Touch the arrow on the **sort by default** button at the top of the screen.
3. Select either:
 - **sort by default**
 - **sort by first name**
 - **sort by last name**
 - **sort by company then first name**
 - **sort by company then last name**
 - **sort by number of SIP URL**

Using Contacts (Address Book) on the BluStar 8000i UI

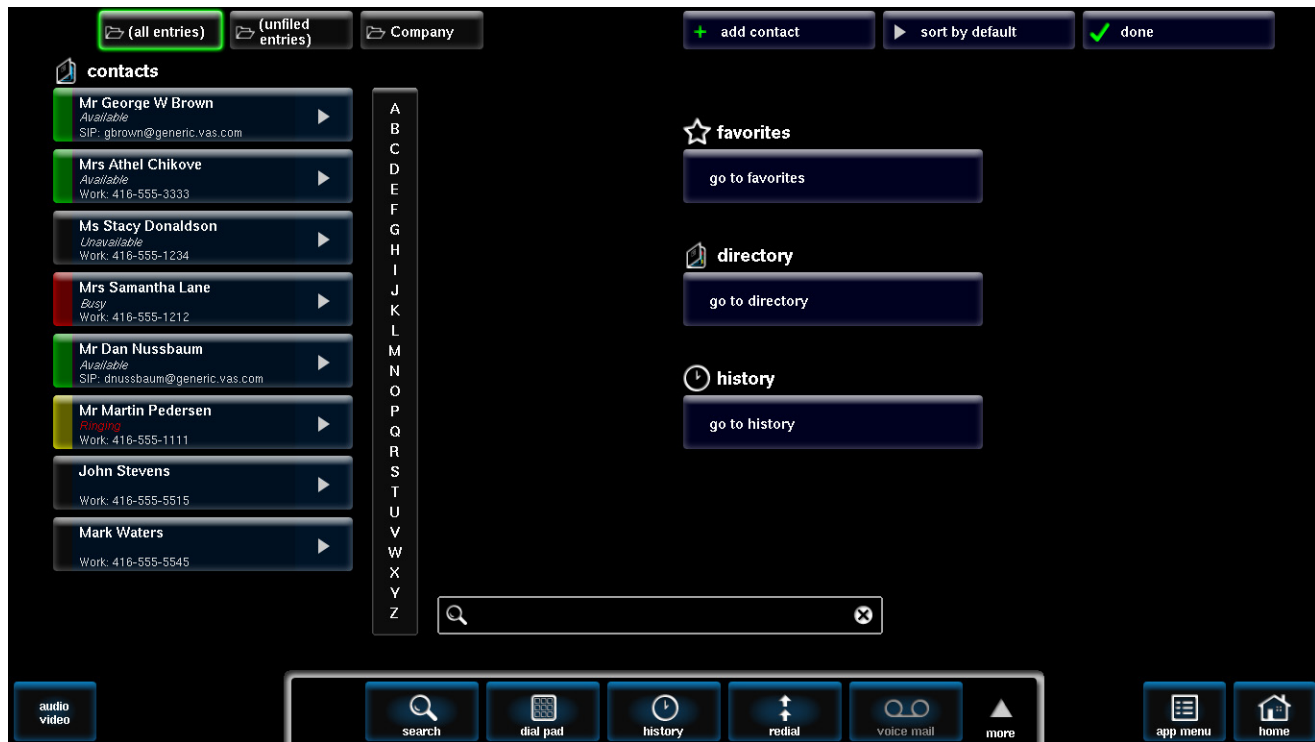
Administrators can populate the user's contacts with the user directory ("**directory 2**") parameter, or you can enable users to import their Microsoft Exchange personal contacts. On the contacts screen on the BluStar 8000i UI, you will see your address book that contains contact buttons, contact folders, an alphabetic menu, a search field, and links to your favorites, directory, and call history. When contacts are sorted by default or by first or last name, you can scroll through them using a A-Z menu.

From the contacts screen, you can manage your address book by doing any of the following:

- search, add, edit, or delete a contact
- select a contact from favorites, directory, and or history menus
- sort contacts
- add a contact to favorites

Contacts are represented as buttons on the screen. A contact button contains the following:

- name of contact
- status (available, busy, ringing, unavailable, see [Busy Lamp Field \(BLF\)](#) on [page 4-37](#) for more information)
- sip address
- arrow to open the contact screen where you can do the following:
 - see the details of the contact
 - change the color of the button
 - dial the contact
- add or delete the contact from your contacts or favorites



To Open the Contacts Screen:

1. In the telephone feature controls, touch the **contacts** button.
The button is outlined in green, indicating that the contacts screen is open.

To Close the Contacts Screen:

1. In the telephone feature controls, touch the **contacts** button to de-select it.
OR
On the contacts screen, touch **done**.
The button is not outlined in green, indicating that the contacts screen is closed.

Searching for a Contact

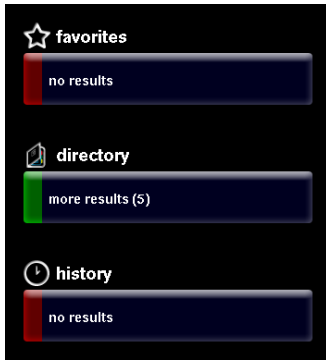
You can search for contacts by going to any of the following:

- Your contacts list (all entries or unfilled entries)
- Favorites
- Directory
- History (call history)

To Search for a Contact:

1. In the telephone feature controls, touch the **contacts** button.
2. Touch either (all entries), (unfiled entries), or a created folder (e.g. Sales).
3. Touch the **search** text field and type in the name of a contact.
4. Touch **search** on the keyboard.
The search results appear under favorites, directory, and history.

5. Touch a button with search results.



6. Touch the arrow on a contact button.
7. Touch + **add to contacts**.
8. Touch **done**.

Configuring the Contact Dynamic Search Threshold

The BluStar 8000i implements a dynamic contact search feature whereby contacts are listed and updated automatically on screen depending on the letters that are typed into the search text field. By default, the dynamic contact search feature is limited to 5000 records. If an LDAP or Exchange directory holds more records than the configured value, users will need to manually touch the **search** button in order to trigger the contact search.

To Configure the Contact Dynamic Search Threshold:

Use the following procedure to configure the contact dynamic search threshold:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Directory Settings](#) on [page A-28](#).

Adding a Contact

You can add a contact from the contacts screen by touching any of the following buttons:

- + add to contacts
- go to favorites
- go to directory
- go to history

You can also import contacts from your Microsoft Exchange personal contacts (see [Microsoft Exchange Contacts](#) on [page 4-30](#))

To Add a New Contact:

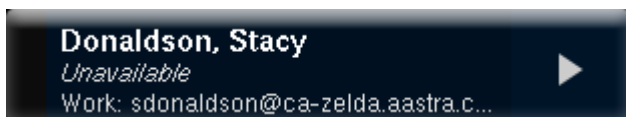
1. In the telephone feature controls, touch the **contacts** button.
2. Touch the + **add contact** button.

3. Enter in the details under the name, numbers, addresses, email/URL, and folders buttons.

4. Touch **done**.

To Add a Contact from Favorites:

1. In the telephone feature controls, touch the **contacts** button.
2. Touch the **go to favorites** button.
3. Touch the arrow on the contacts button.



4. Touch the + **add contact** button.
5. Touch **done**.

To Add a Contact from Directory:

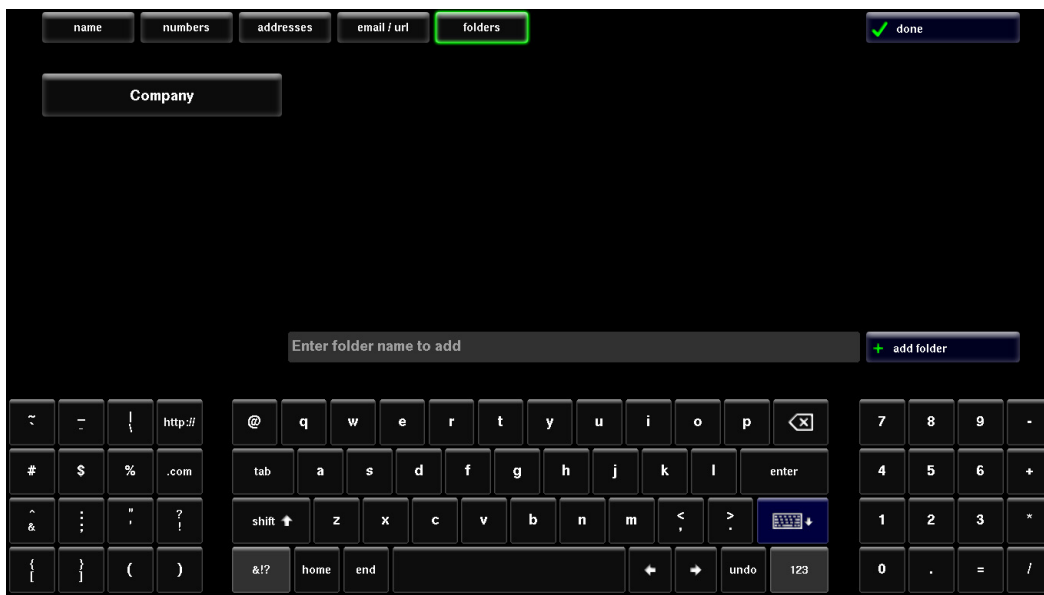
1. In the telephone feature controls, touch the **contacts** button.
2. Touch the **go to directory** button.
3. Touch the arrow on the contacts button.
4. Touch the + **add contact** button.
5. Touch **done**.

To Add a Contact from History:

1. In the telephone feature controls, touch the **contacts** button.
2. Touch the **go to history** button.
3. Touch the arrow on the contacts button.
4. Touch the + **add contact** button.
5. Touch **done**.

To Add a Contact Folder:

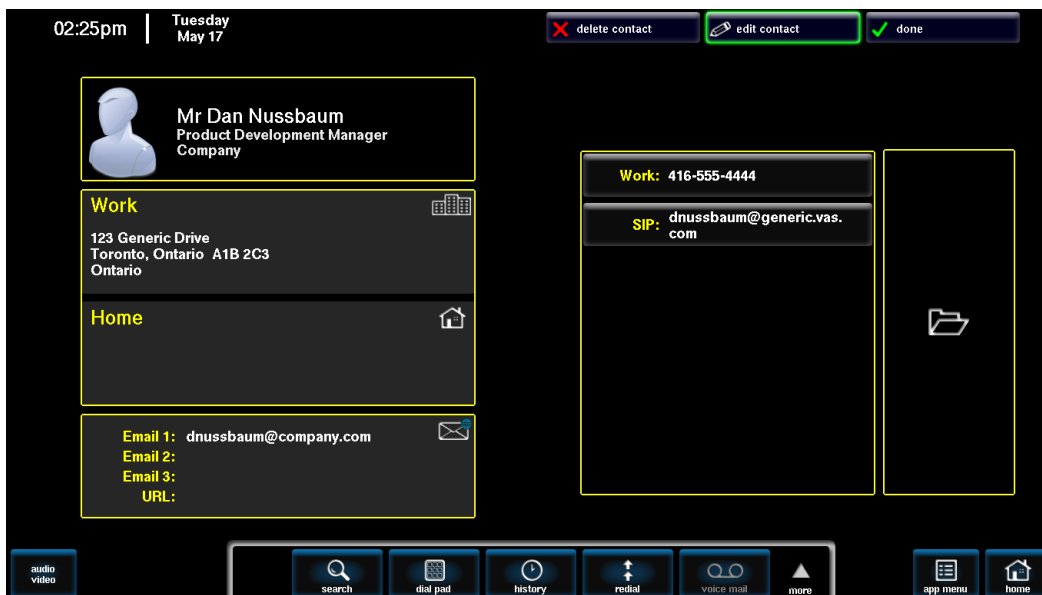
1. In the telephone feature controls, touch the **contacts** button.
2. Touch the **+ add contact** button.
3. Touch the **folders** button.



4. Touch the "Enter folder name to add" text field and type in a new folder name.
5. Touch the **+ add folder** button.
The new folder will appear on the screen.

Editing a Contact

Users can edit a contact's name, address(es), phone number(s), organizational affiliation(s), email/web address(es), and the address book folders where the contact will appear.

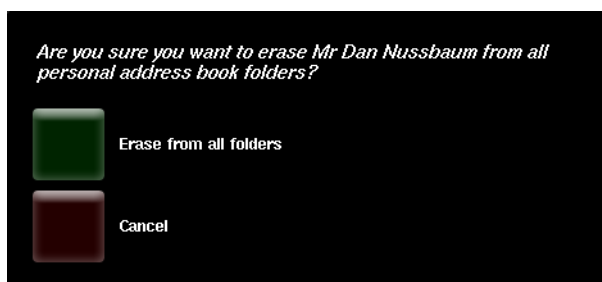


To Edit a Contact:

1. In the telephone feature controls, touch the **contacts** button.
2. Touch the arrow on a contact button to open up the contact's information screen.
3. Touch the **edit contact** button.
All boxes are now outlined in yellow.
4. Touch a box that you want to edit (e.g. Work).
5. Edit the information.
Note:
Do not include the special character "|" in any string that is to be displayed on the BluStar 8000i
6. Touch **done**.

Deleting a Contact

Users can delete a contact from all folders.



To Delete a Contact:

1. In the telephone feature controls, touch the **contacts** button.
2. Touch the arrow on a contact button to open up the contact's information screen.
3. Touch the **x delete contact** button.
You will see the following message: *Are you sure you want to erase Contact from all personal address book folders?*
Note:
If the contact was added as a favorite, the message will also state, "Favorite attached to this contact will also be deleted."
Deleting a contact that has been added as a favorite will automatically delete the corresponding entry in the Favorites menu.
4. Touch **Erase from all folders**.
5. Touch **done**.

Sorting Contact

For each folder you can sort contacts by the following:

- default
- first name
- last name
- company, then first name
- company, then last name
- number or SIP URL

To Sort Contacts:

1. In the telephone feature controls, touch the **contacts** button.
2. Touch a folder button to highlight it.
3. Touch the **sort by default** button.
4. Select the desired sort method.
5. If you do not have to configure anything else on the screen, press **done**.

Basic LDAP Settings

The BluStar 8000i is able to use a Lightweight Directory Access Protocol (LDAP) server for reading directories over an IP network. Administrators can configure LDAP settings using the parameters listed below. If enabled by an Administrator, users can configure their own LDAP settings through their BluStar 8000i terminal. Users can also configure whether to display both the global and LDAP directories on their BluStar 8000i or just the LDAP directory.

LDAP Name

You can specify the name of the LDAP directory using the “**ldap name**” parameter. The name is the label that will be displayed on the directory screen to identify the content, and it is usually the company name or “corporate”.

LDAP Server

You can specify the IP or hostname of the LDAP server using the “**ldap server**” parameter. This will typically be the organization’s main LDAP server, which contains the organization’s main directory (global address book). Users can add additional LDAP servers as desired. This parameter handles multiple values, however the format is the following:

username:password@ldapserver:port

Where:

- username for authentication (optional, if not provided anonymous connection will be used)
- password for authentication (optional)
- ldapserver is the IP address or name of the LDAP server (mandatory)
- port is the LDAP interface port (optional, default is 389)

Example 1: ldap server: ldap.acme.com (no authentication and using default port 389)

Example 2: ldap server: user:password@ldap.acme.com:3268 (authentication and using port 3268)

LDAP Base DN

You can specify the LDAP server base Distinguished Name (DN) or the description of the top level of the directory tree using the “**ldap base dn**” parameter. Usually if a company domain is company.com, the base DN must be entered under the form “dc=company, dc=com”.

For example, ldap base dn: dc=acme, dc=com for acme.com.

User Defined LDAP

The LDAP directory has two sets of settings: Server and User. Server settings are set by the administrator using the parameters above. User settings are configured by the user in the tools menu on the BluStar 8000i UI, and will be stored in the <user.cfg> file.

Note:

User settings override the server settings.

You can allow or disallow the user to edit his or her own LDAP directory configuration that will override the configuration coming from the configuration server using the “**enable user defined ldap**” parameter.

To Configure LDAP Settings:

Use the following procedure to configure LDAP settings:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Basic LDAP Settings on page A-30](#).

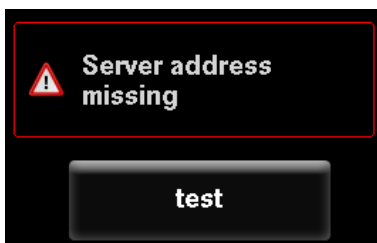
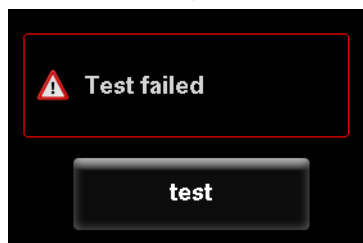
To Configure the LDAP Directory on the BluStar 8000i UI:

1. Touch the **app menu** button, **tools**, then the **LDAP directory** button.
2. Touch the **override server configuration** button.
This allows the user LDAP settings to override the LDAP server settings.
3. Enter the **LDAP directory name**. For example, "acme".
This name will appear as a folder on the directory screen.
4. Enter the **LDAP server** name or IP address. For example, "ldap.company.com".
5. (Optional) Enter the **LDAP port** number. If no port number is entered, the default "389" port will be used.
6. Enter the **LDAP base DN**. For example, "dc=acme, dc=com".
The base DN is the initial filter for every LDAP request.
7. Select **use login credentials** if you want to connect to the LDAP server using the BluStar 8000i user name and password.
OR keep this option unselected and manually enter in a **user name** and **password**.

Note:

If LDAP authentication is anonymous, the user name and password fields can be left empty.

8. Select **only use LDAP directory** if you do not want to use the global directory set up by the system administrator.
9. Touch the test button to test the user settings configuration.
If the configuration is successful, there will be a green check mark above the test button.
If the test failed you will see an error message similar to the ones below.



If you see an error message, go back and re-enter the fields with the correct information.

Advanced LDAP Settings (optional)

When configuring an LDAP directory the option is available to customize the directory using the advanced parameters listed below. These advanced parameters are available for both active and non-active directories unless otherwise stated.

Note:

Advanced LDAP settings are optional and are not required for configuring the BluStar 8000i to use a LDAP server for reading directories over an IP network.

Parameters in Configuration Files	Description
ldap name title attribute list	Specifies the LDAP name title (e.g. Mr.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap name title attribute list: title, gender
ldap first name attribute list	Specifies the LDAP first name (e.g. John) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap first name attribute list: fname, uname
ldap last name attribute list	Specifies the LDAP last name (e.g. Doe) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap last name attribute list: name, lname
ldap middle name attribute list	Specifies the LDAP middle name (e.g. Allen) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap middle name attribute list: mname, initial
ldap name suffix attribute	Specifies the LDAP name suffix (e.g. Ph.D) for the attribute list. If this parameter contains more than one value, only the first matching value will be picked in the record. For example, ldap name suffix attribute: suffix
ldap company attribute list	Specifies the LDAP company name (e.g. Aastra) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap company attribute list: organization, bname
ldap job title attribute list	Specifies the LDAP job title (e.g. Vice President) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap job title attribute list: jtitle, title
ldap business street attribute list	Specifies the LDAP business street (e.g. Snow Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business street attribute list: waddress, baddress
ldap business city attribute list	Specifies the LDAP business city (e.g. Concord) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business city attribute list: wcity, bcity
ldap business state attribute list	Specifies the LDAP business state (e.g. Ontario) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business state attribute list: wstate, bstate
ldap business postal code attribute list	Specifies the LDAP business postal code (e.g. L4K 4N9) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business postal code attribute list: bcode, wcode
ldap business country attribute list	Specifies the LDAP business country (e.g. Canada) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business country attribute list: bcountry, wcountry
ldap home street attribute list	Specifies the LDAP home street (e.g. Internet Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap home street attribute list: hstreet, pstreet
ldap home city attribute list	Specifies the LDAP home city (e.g. Frisco) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap home city attribute list: hcity, pcity
ldap home state attribute list	Specifies the LDAP home state (e.g. Texas) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap home state attribute list: hstate, pstate

Parameters in Configuration Files	Description
ldap home postal code attribute list	Specifies the LDAP home postal code (e.g. 75034) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap home postal code attribute list: hcode, pcode
ldap home country attribute list	Specifies the LDAP home country (e.g. U.S.A) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap home country attribute list: hcountry, pcountry
ldap business phone 1 attribute list	Specifies the LDAP business phone 1 (e.g. 1-905-760-4200) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business phone 1 attribute list: wphone1, bphone1
ldap business phone 2 attribute list	Specifies the LDAP business phone 2 (e.g. 1-905-760-4201) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business phone 2 attribute list: wphone2, bphone2
ldap home phone 1 attribute list	Specifies the LDAP home phone 1 (e.g. 1-416-468-3266) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap home phone 1 attribute list: hphone1, pphone1
ldap home phone 2 attribute list	Specifies the LDAP home phone 2 (e.g. 1-416-468-3267) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap home phone 2 attribute list: hphone2, pphone2
ldap mobile phone attribute list	Specifies the LDAP mobile phone (e.g. 1-416-468-3268) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap mobile phone attribute list: cell, mobile
ldap other phone attribute list	Specifies the LDAP other phone (e.g. 1-416-468-3269) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap other phone attribute list: otherphone, mphone
ldap business fax attribute list	Specifies the LDAP business fax (e.g. 1-905-760-4233) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap business fax attribute list: fax, bfax
ldap email 1 attribute list	Specifies the LDAP email 1 (e.g. john.doe@aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap email 1 attribute list: email1, mail1
ldap email 2 attribute list	Specifies the LDAP email 2 (e.g. john.d@aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap email 2 attribute list: email2, mail2
ldap email 3 attribute list	Specifies the LDAP email 3 (e.g. j.doe@aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap email 3 attribute list: email3, mail3
ldap web address attribute list	Specifies the LDAP web address (e.g. www.aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record. For example, ldap web address attribute list: web, url
ldap cn attribute	Used when both the first and last name of a record are empty. For example, ldap cn attribute: display
ldap dn attribute	Used to perform the search request for the detailed view of an LDAP contact. For example, ldap dn attribute: customDN
ldap dn query mode	Specifies which method to use when an individual record is looked up. If configured as "filter", the BluStar 8000i performs a DN search using the root base DN with the filter "(dn=XXXX)". If configured as "base", the BluStar 8000i performs a DN search using the searched DN as a base with a filter defined in the parameter "ldap dn base query filter" and a scope defined in the parameter "ldap dn base query scope". For example, ldap dn query mode: base Note: This parameter is ignored if the LDAP directory is a Microsoft Active Directory.
ldap dn base query filter	Filter used when an individual record is looked up if the parameter "ldap dn query mode" is set to "base". For example, ldap dn base query filter: (objectClass=*) Note: This parameter is ignored if the LDAP directory is a Microsoft Active Directory.

Parameters in Configuration Files	Description
ldap dn base query scope	<p>Scope used when an individual record is looked up if the parameter "ldap dn query mode" is set to "base". A "base" search is performed only on the base DN, a "onelevel" search is performed on the base DN and the first sublevel, and a "subtree" search is performed on the whole tree under the base DN. For example, ldap dn base query scope: onelevel</p> <p>Note: This parameter is ignored if the LDAP directory is a Microsoft Active Directory.</p>
ldap search filter	<p>Used to set search filters. This parameter format must follow RFC 4515, for example (sn=%). This parameter must include a '%' character at the place where it will be replaced by a*, b*, etc...</p> <p>For example, ldap search filter: (&(sn=*)(number=*))</p>
ldap search scope	<p>Used to set the search scope. A "base" search is performed only on the baseDN, a "onelevel" search is performed on the baseDN and the first sublevel, and a "subtree" search is performed on the whole tree under the base DN.</p> <p>For example, ldap search scope: onelevel</p>
ldap search timeout	<p>Used to set the request timeout for LDAP requests. A range of 1 to 120 is applicable.</p> <p>For example, ldap search timeout: 30</p>
ldap network timeout	<p>Used to set the network timeout for LDAP requests. A range of 1 to 120 is applicable.</p> <p>For example, ldap network timeout: 50</p>
ldap initial download delay	<p>Used to set the LDAP initial download delay. Setting a value of 0 does not introduce any delay and the initial download is performed synchronously during the login process. With all other values, the download is performed asynchronously, delayed by the value amount (in seconds) after the login process. A range of 0 to 120 is applicable.</p> <p>For example, ldap initial download delay: 60</p>

To Configure Advanced LDAP Settings:

Use the following procedure to configure advanced LDAP settings:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Advanced LDAP Settings](#) on [page A-32](#).

Microsoft Exchange Contacts

Users can import their Microsoft Exchange contacts into their BluStar 8000i address book. This allows users to stay in sync with their business contacts. Any changes (i.e. users create, modify, or delete contacts) made to contacts on the BluStar 8000i and/or on the PC will automatically update the Microsoft Exchange contacts in real time. Users can also use Secure Sockets Layer (SSL), which provides secure communications over the Internet. All data exchanged is also encrypted to increase security.

Note:

If users import Microsoft Exchange personal contacts, they will not have access to their user directory set by the “directory 2” parameter.

To Configure User Defined Exchange Contacts Settings:

The following parameters can be used to configure the user-defined Microsoft Exchange contacts settings:

Parameters in Configuration Files	Description
enable user defined exchange contacts	Specifies whether to enable or disable a user's ability to edit his or her Microsoft Exchange contacts configuration. For example, enable user defined exchange contacts: 1
exchange contacts enabled	Specifies whether a user's Microsoft Exchange contacts should be synced with the terminal's address book. When enabled, the user will not be able to access the personal contacts that have been set up by the administrator. For example, exchange contacts enabled: 1
exchange email	Specifies the user's Microsoft Exchange email address. For example, exchange email: john.doe@acme.com
exchange server ip	Specifies the user's Microsoft Exchange server IP address or Fully Qualified Domain Name (FQDN). For example, exchange server ip: mail.acme.com
exchange user domain	Specifies the user's Microsoft Exchange domain name. For example, exchange user domain: acme
exchange contact folder name	Specifies the optional custom folder that will be used to store the user's Microsoft Exchange contacts. For example, exchange contact folder name: Exchange
exchange use login credentials	Specifies whether the user's BluStar 8000i user name and password is the same the user's Microsoft Exchange user name and password (enabled) or if login credentials should be manually input (disabled). For example, exchange use login credentials: 1
exchange username	Specifies the user's Microsoft Exchange user name. This parameter is only used if the parameter “exchange use login credentials” is set to disabled. For example, exchange username: jdoe
exchange password	Specifies the user's Microsoft Exchange password. This parameter is only used if the parameter “exchange use login credentials” is set to disabled. Note: The “exchange password” parameter is available in the user.cfg file, but the password string will be encrypted. The password can only be input by the user through the contacts menu on the user's respective BluStar 8000i terminal.
exchange ssl enabled	Specifies whether SSL (Secure Sockets Layer) should be enabled or disabled. For example, exchange ssl enabled: 1

Use the following procedure to configure the user-defined Microsoft Exchange contacts settings.

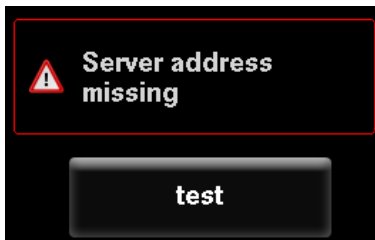
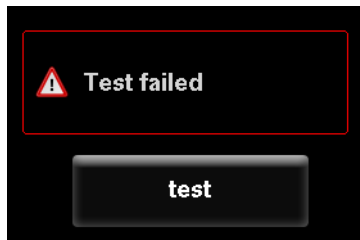


Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Microsoft Exchange Contact Settings](#) on page A-44.

To Configure the Microsoft Exchange Contacts on the BluStar 8000i UI:

1. Touch the **app menu** button, **tools**, then the **contacts** button.
2. Touch the **use Microsoft Exchange personal contacts** button.
Note:
 When you select this option you won't be able to access your personal contacts that have been set up by your administrator.
3. Enter your **Microsoft Exchange email** address. For example, "johndoe@acme.com".
4. Enter the **Microsoft Exchange server** name or IP address. For example, "mail.acme.com".
5. Select **use custom folder name** and enter the **contact folder name** if you want to create a custom folder for your Microsoft Exchange contacts.
6. Select **use login credentials** if your BluStar 8000i user name and password is the same as your Microsoft Exchange user name and password.
 OR keep this option unselected and manually enter in your Microsoft Exchange **username**, (optional) **domain**, and **password**.
7. Select **use SSL** (Secure Sockets Layer) if you want to ensure that you have secure communications over the Internet.
8. Touch the **test** button to test the configuration.
 If the configuration is successful, there will be a green check mark above the test button (see image above).
 If the test failed, you will see an error message similar to the ones below.



If you see an error message, go back and re-enter the fields with the correct information.

LDAP Directory/Exchange Contacts Update Interval

Configuration parameters are available that allow administrators the ability to configure detailed update schedules for the LDAP directory and Exchange contacts. These parameters include:

Parameter in Configuration Files	Description
LDAP Directory	
ldap resync time	Sets the time of day in a 24-hour period for the BluStar 8000i terminal to automatically update the LDAP directory. Example: ldap resync time: 03:15
ldap resync days	Specifies the amount of days that the terminal waits between resync operations for the LDAP directory. Example: ldap resync days: 1
ldap resync max delay	Specifies the maximum time, in minutes, the terminal waits past the scheduled time before starting a resync for the LDAP directory. Example: ldap resync max delay: 60
Exchange Contacts	
exchange contacts resync time	Sets the time of day in a 24-hour period for the BluStar 8000i terminal to automatically update the Exchange contacts. Example: exchange contacts resync time: 03:15
exchange contacts resync days	Specifies the amount of days that the terminal waits between resync operations for the Exchange contacts. Example: exchange contacts resync days: 1
exchange contacts resync max delay	Specifies the maximum time, in minutes, the terminal waits past the scheduled time before starting a resync for the Exchange contacts. Example: exchange contacts resync max delay: 60

Notes:

- Resync time is based on the local time of the terminal.
- Resync will occur any time between the values set for the "[ldap/exchange contacts] resync time" and "[ldap/exchange contacts] resync max delay" parameters. For example, if the "ldap resync time" parameter is set to 02:00 and the "ldap resync max delay" is set to 30, the LDAP directory update will take place any time between 02:00 and 02:30.

To Configure the LDAP Directory/Exchange Contacts Update Interval:

Use the following procedure to configure the LDAP directory/exchange contacts update interval:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [LDAP Directory/Exchange Contacts Update Interval](#) on page A-47.

Voicemail

Pressing the voicemail button on the BluStar 8000i allows a user to directly dial their voicemail and access their messages. Administrators can setup the voicemail feature using the configuration files. The BluStar 8000i phone displays up to 99 voicemail messages for an account even if the number of voicemail exceeds the limit.

Message Indicator

The voicemail button will show a message indicator that increments the number of new voicemail messages. In SIP Call Server mode, a (!) may display instead of a number to indicate that there is a new voicemail.



Once a user touches the voicemail button to listen to the messages, the message indicator will disappear from the button.

To Configure Voicemail:

You can setup voicemail in the configuration files using the “**sip vmail**” parameter to dial a specific number to access an existing voicemail account. The user then follows the voicemail instructions for listening to voicemails.

Use the following procedure to enable/disable voicemail:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Voicemail Settings on page A-68](#).

Note:

The SIP account used on the BluStar 8000i must have a configured voicemail box.

Using Voicemail on the BluStar 8000i UI:

1. On the BluStar 8000i UI, touch the **voicemail** button.
You will be connected to a voicemail server where you can enter in your password to retrieve your messages.

Note:

If the video voicemail client feature is configured on the respective BluStar 8000i terminal, pressing the telephone feature controls voicemail button initiates the video voicemail client instead of connecting you directly to your voicemail server. Refer to [Video Voicemail Client Integration on page 4-34](#) for more information.

Video Voicemail Client Integration

The BluStar 8000i video voicemail client organizes voicemail messages into a simple-to-use and easy-to-access list. Users can view all pertinent details with regards to their voicemail messages (e.g. sender name, phone number, date and time received, message duration, etc.) and manage all voicemail duties (e.g. play, delete, callback, etc.) using the intuitive controls on their touchscreen. A multitude of voicemail account settings can also be easily configured through the video voicemail client.

Note:

The availability of the video voicemail client integration feature is dependant on your call manager. Please contact the system administrator for your respective call manager for feature availability details.

Administrators can configure the respective BluStar 8000i terminals for use with the video voicemail client by defining the following parameters in the configuration files:

Parameter in Configuration Files	Description
voicemail integration url	The url (http or https) the BluStar 8000i calls to perform voicemail integration. Example: voicemail integration url: http://myserver.com/integration.php
voicemail integration use login credentials	By default the BluStar 8000i uses SIP credentials to authenticate (digest method) to the voicemail integration server. Enabling this configuration parameter makes the BluStar 8000i use the user login/password instead. Example: voicemail integration use login credentials: 1
voicemail integration needs sip registration	Used by the voicemail integration API to indicate to the software if SIP registration is needed before sending a user command via the API. When enabled, the BluStar 8000i checks the extension registration status before sending an API command. If the extension is not registered, an error message is displayed. Example: voicemail integration needs sip registration: 1

Note:

In addition to the above parameters, please ensure that “sip xml notify event” is enabled. For more information, refer to [XML SIP Notify Events](#) on [page 5-4](#).

Configuring Video Voicemail Client Integration

Use the following procedure to configure video voicemail client integration on the BluStar 8000i:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Video Voicemail Client Integration Settings](#) on [page A-69](#).

Emergency Dial Plan

Public telephone networks in countries around the world have a single emergency telephone number (emergency service number) that allows a caller to contact local emergency services for assistance when required. The emergency telephone number may differ from country to country. It is typically a three-digit number so that it can be easily remembered and dialed quickly. Some countries have a different emergency number for each of the different emergency services.

You can specify the digits to dial on the BluStar 8000i for contacting emergency services. Once you specify the emergency number(s) on the terminal, you can dial those numbers directly on the dial pad when the terminal is locked and the terminal will automatically dial to the specified emergency service.

Note:

Contact your local phone service provider for available emergency numbers in your area.

The following table describes the default emergency numbers on the BluStar 8000i.

Emergency Number	Description
911	A United States emergency number
999	A United Kingdom emergency number
112	An international emergency telephone number for GSM mobile phone networks. In all European Union countries it is also the emergency telephone number for both mobile and fixed-line telephones.
110	A police and/or fire emergency number in Asia, Europe, Middle East, and South America.

Emergency Dial Plan and Pattern Matching

The BluStar 8000i supports emergency dialing using pattern matching and prepend dial plan functionality.

There are two ways to dial a number on the terminal:

- dialing digit-by-digit (i.e. select line and dial)
- dialing by string (i.e. pre-dial then go off-hook)

When a user dials digit-by-digit, the terminal adds every digit to a dialed string and checks against the dial plan. If the terminal is not locked, it checks against the regular dial plan. If the terminal is locked, it checks against the emergency dial plan.

When a user dials by string, (pre-dial, speed-dial, etc., and then goes off-hook), and the terminal is not locked, it checks to see if the number matches the emergency dial plan. If it does not match, it blocks the call from going through. If the terminal is locked, and the number matches the emergency dial plan it allows the call to go through.

Adding a prepend to a dial plan also works with both dialing digit-by-digit and dialing by string.

Limitation

A secondary dial tone is not supported for emergency dial plans with pattern matching.

Configuring an Emergency Dial Plan

Use the following procedure to configure an emergency dial plan.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Emergency Dial Plan Settings](#) on page A-70.

Picture ID Feature

The Picture ID feature on the BluStar 8000i shows a picture ID of a caller on the LCD for all of the following events:

- Incoming calls (matched to caller ID numbers)
- Outgoing calls (matched to dialed numbers)
- Directory entries
- Callers list entries
- Redial list entries

The pictures are stored in a centralized picture repository and are dynamically retrieved from the centralized server for each call and then locally cached in the BluStar 8000i to reduce network traffic.

If there is no picture on the central server for the dialed and/or caller ID number, directory, callers list, and/or redial list entry, the generic blue figure image is shown.

Pictures can be in either “png”, “gif”, or “jpeg” formats, but must be named “.png”, up to 320 pixels wide x 320 pixels tall, and in 24 bit color.

The filenames for pictures must be stored using the phone number as the filename using only digits (for example, 9995551234.png).



**Generic
Blue Image**

Note:

The picture ID feature supports the use of FTP, HTTP, and HTTPS protocols when downloading pictures.

To Enable/Disable Picture ID:

Enabling the picture ID feature on the BluStar 8000i can be done using the “**image server uri**” parameter. Entering no value for this parameter disables the feature. The parameter format is the following:

image server uri: protocol://[username]:[password]@server.[port]

Use the following procedure to enable the picture ID feature.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Picture ID Feature on page A-75](#).

Busy Lamp Field (BLF)

The BLF feature on the BluStar 8000i allows users to monitor their favorite contacts (speed dial list) for state changes. BLF monitors the status (available [green], ringing [yellow], busy [red], and unavailable [black]) of extensions on the BluStar 8000i.

Example

A supervisor has a worker added to her favorites and she configures BLF on her BluStar 8000i for monitoring the status of the worker's BluStar 8000i use (busy, ringing, available, and unavailable). When the worker picks up his BluStar 8000i to make a call, the contact button goes red (busy) on the supervisor's BluStar 8000i favorites screen to show that the worker's phone is in use.

BLF Setting

(For use with Asterisk)

The busy, available, and unavailable state is monitored for other BluStar 8000i configured on the Asterisk server. When the monitored user is available, the contact button is green and says *Available*. When the monitored user is on an active call, the contact button is red and says *Busy*. When the user is unavailable, the contact button is black and says *Unavailable*.

BLF/List Setting

(For use with the BroadSoft Broadworks Rel 13 or higher platforms only)

The BLF/List feature on the BluStar 8000i is specifically designed to support the BroadSoft Broadworks Rel 13 Busy Lamp Field feature. This feature allows the BluStar 8000i to subscribe to a list of monitored users defined through the BroadWorks web portal.

In addition to monitoring the available, unavailable, and busy state, the BLF/List feature also supports the ringing state. When the monitored user is available, the contact button is green and says *Available*. When the monitored user is in a ringing state, the contact button is yellow and says *Ringing*. When the monitored user is on an active call, the contact button is red and says *Busy*. When the user is unavailable, the contact button is black and says *Unavailable*.

You can specify the BLF list URI that the BluStar **8000i** uses to access the required BLF list using the "**list uri**" parameter in the configuration files.

Configuring BLF/List Setting

Use the following procedure to configure the BLF/List setting:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [BLF List URI Settings](#) on page A-75.

BLF Subscription Period

On the BluStar 8000i, you can set the amount of time, in seconds, that the BluStar 8000i will attempt to subscribe to the BLF subscription service after a user logs in to his/her account. The BluStar 8000i will attempt to subscribe to the BLF subscription service before the defined subscription period ends. In the configuration files, enter the following parameter with a valid value to set the BLF subscription period:

sip blf subscription period: <value in seconds>

The minimum value for this parameter is 120 seconds (2 minutes). The default value is 3600 seconds (1 hour). If you enter a value lower than 120 for this parameter, the default value (3600) will be used by the BluStar 8000i.

Configuring BLF Subscription Period

Use the following procedure to configure the BLF subscription period on the BluStar 8000i:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [BLF Subscription Period Settings](#) on page A-76.

Directed Call Pickup

Directed call pickup is a feature on the BluStar 8000i that allows a user to intercept a call on a ringing BluStar 8000i that is part of the same interception group. You can use the directed call pickup feature with the existing BLF feature. You can specify the directed call pickup feature by using the **“directed call pickup”** parameter in the configuration files.

With Asterisk, a user can dial *76 followed by the extension to pick up a ringing call on another BluStar 8000i. For more information about BLF, see [Busy Lamp Field \(BLF\)](#) on page 4-37.

Note:

The Asterisk and Epygi Quadro 4x/16x IP PBX servers support this feature. For details about Asterisk support, contact Aastra Technical Support.

Directed Call Pickup Prefix (optional)

The optional **“directed call pickup prefix”** parameter allows you to enter a specific prefix string (depending on what is available on your server), that the BluStar 8000i automatically dials when dialing the directed call pickup number.

For example, for Broadsoft servers, you can enter a value of *97 for the **“directed call pickup prefix”** parameter. When the BluStar 8000i performs the directed call pickup after a user presses a BLF or BLF/List softkey, the BluStar 8000i prepends the *97 value to the designated extension of the BLF or BLF/List softkey when dialing out.

How this feature works when Directed Call Pickup is enabled with BLF or BLF/List

1. BluStar A monitors BluStar B via BLF/List.
2. BluStar C calls BluStar B; BluStar B rings.
3. If you press the BLF/List softkey on BluStar A, it picks up the ringing line on BluStar B.
4. BluStar C connects to BluStar A.

How this feature works when Directed Call Pickup is disabled with BLF or BLF/List

1. BluStar A monitors BluStar B via BLF/List.
2. BluStar C calls BluStar B; BluStar B rings.
3. If you press the BLF/List softkey on BluStar A, it performs a speed dial to BluStar B.
4. BluStar C and BluStar A are ringing BluStar B on separate lines (if available).

Notes:

- The default method for the BluStar 8000i to use is directed call pickup over BLF if the server provides applicable information. If the directed call pickup over BLF information is missing in the messages to the server, the directed call pickup by prefix method is used if a value for the prefix code exists in the configuration.
- You can define only one prefix at a time for the entire BLF/List.
- The BluStar 8000i that picks up the call displays the prefix code + the extension number (for example, *971234 where prefix key = *97, extension = 1234).

Configuring Directed Call Pickup

Use the following procedure to enable or disable the directed call pickup feature on the BluStar 8000i:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Directed Call Pickup](#) on [page A-76](#).

Configuring BL F/BLF List for Directed Call Pickup

Use the following procedure to configure BLF/BLF List for directed call pickup:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [BLF List URI Settings](#) on [page A-75](#).

Diversión Display

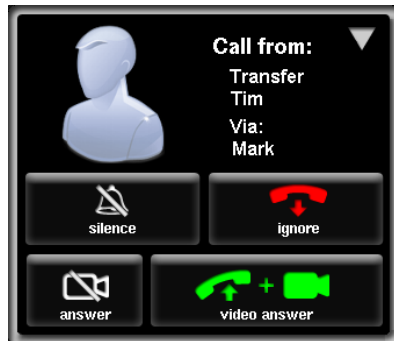
When an outgoing call from the BluStar 8000i is being diverted to another destination (i.e., via call forward), the BluStar 8000i displays the caller ID (display name and username) of the new destination and the reason for the call diversion. Similarly, at the new destination, the caller ID of the original call destination displays.

Call Diversion Example:

1. Tim calls Mark at x400.
2. Mark's BluStar 8000i is busy.
3. Mark's BluStar 8000i diverts the incoming call to another destination (Mark has immediate call forwarding set to Roger @ ext. 464).
4. Tim's BluStar 8000i displays the name and extension of where the call is being diverted to and the reason for diverting the call.



5. Roger's BluStar 8000i accepts the call and displays the name (or number) of the BluStar 8000i of the incoming call (Tim) and the name (or number) of the original destination (Mark).



Note:

If proxy servers exist in the network, it is possible that multiple diversions can take place on the BluStar 8000i. When multiple diversion headers are returned in a single 302 response back to the originating BluStar 8000i, the BluStar 8000i that originated the call (i.e., Tim's BluStar 8000i in above example) displays the URI of the newest (first encountered) Diversion header, but displays the REASON of the oldest (last encountered) Diversion header. The BluStar 8000i that receives the diverted call (i.e., Roger's BluStar 8000i in example above) displays the information of the oldest diverted call (last encountered).

Limitations

- The Diversion header assumes that the ID of the 'diverted' caller is passed in a URI style manner.
- This feature relies on the server supporting and generating the diversion header; the BluStar 8000i does not generate the header itself.
- The diversion header parameters (i.e., counter, limit, privacy, screen, and extension) are not recognized or supported by the BluStar 8000i. However, they are still passed along during the diversion process.

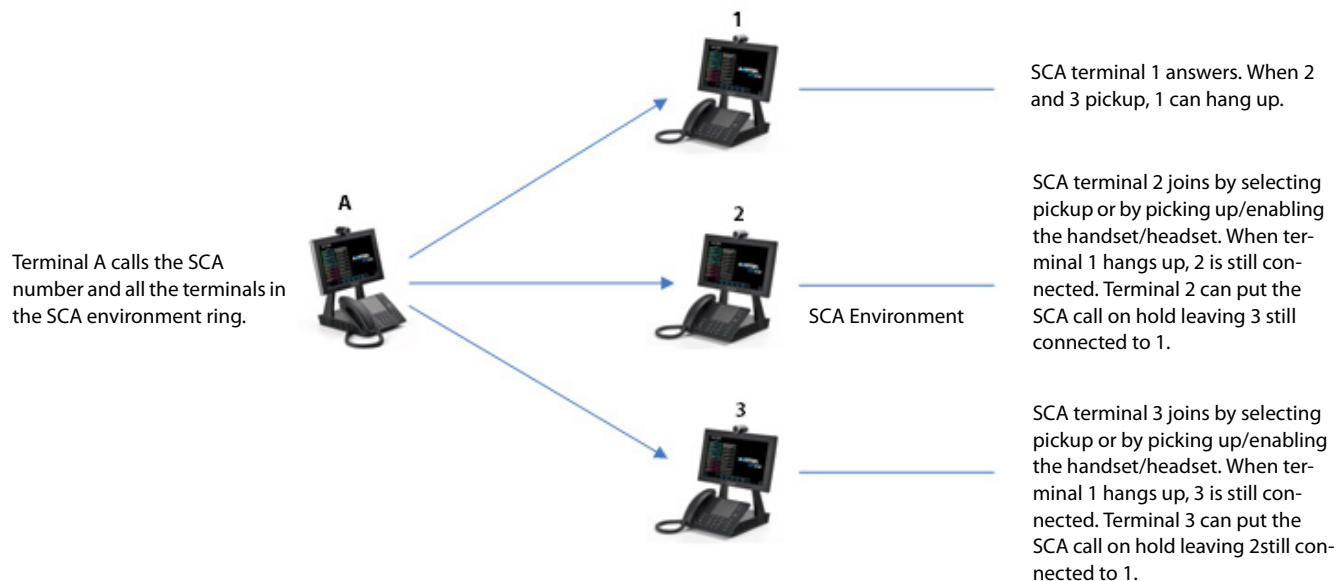
Shared Call Appearance (SCA) and SCA Call Bridging

Shared Call Appearance (SCA) is a feature where incoming calls are presented to multiple terminals simultaneously. A use case scenario can be seen in situations where an executive's line is available to be handled on the executive's BluStar 8000i terminal and by the executive's assistant on the assistant's BluStar 8000i terminal. It is also useful in general situations where there is a need to handle incoming calls on a main line from multiple locations.

Calls can be transferred between two terminals that share a SCA line by simply putting the call on hold at one terminal and picking it up on the other. Line status changes are reflected on each respective terminal in unison, allowing all people sharing the line to see the status at a glance.

The BluStar 8000i also includes an enhanced SCA for servers that support call bridging and allows two or more SCA users to be connected in a call with a third party.

Refer to the following example:



Using the example above, when a call comes into terminal 1, terminal 2 and terminal 3 can join the same call either by touching the pickup icon in the expanded call appearance bar or by picking up/enabling the handset/headset. Existing SCA parties in a bridge or one-to-one call hear an audible beep when another party joins the call.

Note:

Enabling/disabling the beep is configurable on the server-side.

If a terminal is configured for SCA bridging but the account on the server does not have this functionality enabled the pickup option will not be available. Additionally, if the handset is picked up, a message will be displayed stating the line is in use.

The SCA call bridging feature is disabled by default on all terminals. You can enable this feature using the configuration files only. Administrators can configure BluStar 8000i terminals for use with SCA and SCA call bridging by utilizing the following parameters:

Parameters in Configuration Files	Description
sip mode	The mode-type that you assign to the BluStar 8000i. Valid values are Generic (0), BroadSoft SCA (1), Reserved for (2), or BLA (3). Default is Generic (0). For example, sip mode: 1
sip sca bridging	Enables/disables SCA bridging on the terminal-side on a global basis. For example, sip sca bridging: 1

To Configure SCA Lines Using the Configuration Files:

Use the following procedure to enable/disable the SCA feature on the BluStar 8000i:

**Configuration Files**

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Shared Call Appearance \(SCA\) Call Bridging](#) on page A-25.

XML Settings

Extensible Markup Language (XML) is a markup language much like HTML. HTML was designed to display data and to focus on how data looks. XML was designed to describe data and to focus on what data is.

The following are characteristics of XML:

- XML tags are not predefined. You must define your own tags
- XML uses a Document Type Definition (DTD) or an XML Schema to describe the data
- XML with a DTD or XML Schema is designed to be self-descriptive
- XML is a W3C Standard Recommendation

XML Get Timeout

The BluStar 8000i has a parameter called, “**xml get timeout**” that allows you to specify a timeout value, in seconds, that the BluStar 8000i waits for the far side to return a response after accepting the HTTP GET connection. If the far side accepts the GET connection but never returns a response, it blocks the BluStar 8000i until it is rebooted.

The default is “0” (never timeout). If you enter a value greater than “0” for this parameter, the BluStar 8000i times out and will not be blocked.

Configuring XML Get Timeout

Use the following procedure to configure the XML Get Timeout feature on the BluStar 8000i:

**Configuration Files**

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [XML Settings](#) on page A-77.

Licensing

Licenses can be obtained that will allow users to utilize additional features on the BluStar 8000i. Licenses are available for the following BluStar 8000i features:

Feature	Description
G.729	License to integrate G.729 codec functionality. G.729 is a multi-purpose ITU-T standard for increased bandwidth availability and short delay (coding of speech at 8 kbit/s using CS-ACELP).
VPN	License to integrate VPN functionality. The BluStar 8000i integrates an OpenVPN client for authentication and remote access to the corporate network. OpenVPN is a highly-flexible open-source VPN application available for a multitude of operating systems that utilizes SSL/TLS for key exchange. Utilizing OpenVPN Access Server, administrators can set up and configure their networks to allow remote terminals access to the corporate network ensuring that all the conferencing and collaboration capabilities of the BluStar 8000i can be fully utilized in a remote environment.
Note: See Virtual Private Network (VPN) on page 3-10 for more information.	

Note:

Please contact your respective Aastra representative for information on obtaining licenses.

To Install Licenses:

1. Place the license file(s) on your configuration server.
2. Restart the affected BluStar 8000i terminals as described in [Logging Off / Restarting](#) on [page 1-14](#).
3. Ensure the licenses are enabled by viewing the **Licensed Features** information through the **status** app.

Chapter 5

Advanced Operational Features

The BluStar 8000i has specific advanced operational features that you can configure. This chapter describes each feature and provides procedures for configuring a BluStar 8000i to use these features.

Advanced Operational Features

This section provides information about the following advanced features on the BluStar 8000i:

- [Update Caller ID During a Call](#)
- [MAC Address in REGISTER Messages](#)
- [SIP Message Sequence for Blind Transfer](#)
- [Removing UserAgent and Server SIP Headers](#)
- [Removing Inactive Video Streams in the SDP](#)
- [Blacklist Duration](#)
- [Whitelist Proxy](#)
- [XML SIP Notify Events](#)
- [Configurable DNS Queries](#)
- [Ignore Out of Sequence Errors](#)
- [Switching Between Early Media and Local Ringing](#)
- [Configurable “Allow” and “Allow-Event” Optional Headers](#)
- [Configurable SIP P-Asserted Identity \(PAI\)](#)
- [Configurable Compact SIP Header](#)
- [Configurable Dial Plan Terminator](#)

Update Caller ID During a Call

It is possible for a proxy or call server to update the caller ID information that displays on the BluStar 8000i during a call, by modifying the SIP Contact header in the re-INVITE message. The BluStar 8000i displays the updated name and number information contained within the Contact header. The **“sip update callerid”** parameter allows the system administrator to enable or disable this feature.

Configuring Update Caller ID During a Call

Use the following procedure to configure the update caller ID feature during a call.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Update Caller ID Setting on page A-78](#).

MAC Address in REGISTER Messages

The BluStar 8000i can send the MAC address in the REGISTER packets making it easier for the call server when a user configures the BluStar 8000i. The following configurable header sends this information to the call server:

```
Aastra-Mac: <mac address>
```

The MAC address is sent in uppercase hex numbers, for example, 00085D03C792. The “**sip send mac**” parameter allows you to enable/disable the sending of MAC address to the call server. The parameter is disabled by default.

Configuring the MAC address in REGISTER Message

Use the following procedure to configure the MAC address in the REGISTER message:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Shared Call Appearance \(SCA\) Call Bridging](#) on page A-25.

SIP Message Sequence for Blind Transfer

The SIP message sequence for blind transfer avoids the transfer target having two simultaneous calls. A CANCEL message is sent to the transfer target (if it is in a ringing state) before sending a REFER to the transferee to complete the transfer. The “**sip cancel after blind transfer**” parameter allows the system administrator to force the BluStar 8000i to use the blind transfer method.

Configuring SIP Message Sequence for Blind Transfer

Use the following procedure to configure the SIP message sequence for blind transfer:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Blind Transfer Setting](#) on page A-78.

Removing UserAgent and Server SIP Headers

The BluStar 8000i always configures the SIP UserAgent/Server headers to contain:

```
Aastra <PhoneModel>/<FirmwareVersion>
```

You can suppress the addition of these headers by using the “**sip user-agent**” parameter in the configuration files. Setting this parameter allows you to enable or disable the addition of the User-Agent and Server SIP headers from the SIP stack.

Configuring UserAgent/Server SIP Headers

Use the following procedure to configure the user agent/server SIP headers:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [User-Agent Settings](#) on page A-78.

Removing Inactive Video Streams in the SDP

The configuration parameter, “remove inactive video stream”, can be used to remove the video stream from the SDP in situations where the video stream should be disabled but the audio stream should be kept active. This parameter is disabled by default.

Configuring the Inactive Video Stream SDP Removal Feature

Use the following procedure to configure the inactive video stream SDP removal feature:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Inactive Video Stream Settings](#) on page A-79.

Blacklist Duration

The Blacklist Duration feature helps to reduce unnecessary delays during proxy/registrar server failures, caused by the BluStar 8000i repeatedly sending SIP messages to a failed server. If you enable this feature, whenever the BluStar 8000i sends a SIP message to a server and does not get a response, the BluStar 8000i automatically adds the server to the blacklist. The BluStar 8000i avoids sending messages to any servers on the blacklist. If all servers are on the blacklist, then the BluStar 8000i attempts to send the message to the first server on the list.

You can specify how long failed servers remain on the blacklist in the BluStar 8000i's configuration file. The default setting is '300' seconds (5 minutes). If you set the duration to '0' seconds, then you disable the blacklist feature.

Configuring Blacklist Duration Using the Configuration Files

Use the following procedure to configure the blacklist duration:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Blacklist Duration Setting](#) on page A-79.

Whitelist Proxy

To protect your BluStar 8000i network, you can configure a **Whitelist Proxy** feature that screens incoming call requests received by the BluStar 8000i. When this feature is enabled, an BluStar 8000i accepts call requests from a trusted proxy server *only*. The BluStar 8000i rejects any call requests from an untrusted proxy server

Configuring Whitelist Proxy Using the Configuration Files

Use the following procedure to configure the whitelist proxy feature:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Whitelist Proxy Setting](#) on page A-79.

XML SIP Notify Events

In order for an XML push to bypass the NAT/firewall, the BluStar 8000i supports a proprietary SIP NOTIFY event (astra-xml) with or without XML content. An administrator can enable/disable the SIP NOTIFY event using the “**sip xml notify event**” parameter.

If XML content is provided in the SIP NOTIFY, it is processed directly by the BluStar 8000i as it is done for an XML PUSH. If the content is empty in the SIP NOTIFY, the BluStar 8000i automatically triggers a new pre-configured action uri (action uri xml sip notify).

Example of a SIP NOTIFY with XML Content

```
NOTIFY sip:200@10.30.100.103:5060 SIP/2.0
Via: SIP/2.0/UDP 10.30.100.103:5060;branch=z9hG4bK7bbc1fac;rport
From: <sip:201@10.30.100.103:5060>;tag=81be2861f3
To: Jacky200 <sip:200@10.30.100.103:5060>
Contact: <sip:201@10.30.100.103>
Call-ID: 59638f5d95c9d301
CSeq: 4 NOTIFY
Max-Forwards: 70
Event: aastra-xml
Content-Type: application/xml
Content-Length: 115
<AastraBluStar>
<dnd>
<status>1</status>
</dnd>
</AastraBluStar>
```

When the BluStar 8000i receives the SIP NOTIFY, the XML content is processed as any XML object. In the above example, the BluStar 8000i calls `http://10.30.100.39/XMLtests/SampleTextScreen.xml` after reception of the SIP NOTIFY.

Example of a SIP NOTIFY without XML Content

```
NOTIFY sip:200@10.30.100.103:5060 SIP/2.0
Via: SIP/2.0/UDP 10.30.100.103:5060;branch=z9hG4bK7bbc1fac;rport
From: <sip:201@10.30.100.103:5060>;tag=81be2861f3
To: Jacky200 <sip:200@10.30.100.103:5060>
Contact: <sip:201@10.30.100.103>
Call-ID: 59638f5d95c9d301
CSeq: 4 NOTIFY
Max-Forwards: 70
Event: aastra-xml
Content-Type: application/xml
Content-Length: 0
```

When the BluStar 8000i receives the SIP NOTIFY, it will trigger the “**action uri xml sip notify**” parameter, if it has been previously configured using the configuration files. If the “**action uri xml sip notify**” parameter is not configured, the BluStar 8000i does not do anything. On the phone side, a system administrator can enable or disable this SIP NOTIFY feature using the configuration files. Also to ensure that the SIP NOTIFY is coming from a trusted source, it is recommended that you enable the [Whitelist Proxy](#) feature (“**sip whitelist**” parameter) on the BluStar 8000i. If enabled, and the BluStar 8000i receives a SIP NOTIFY from a server that is NOT on the whitelist, the BluStar 8000i rejects the message.

Enabling/Disabling XML SIP NOTIFY Using the Configuration Files

To enable/disable the SIP NOTIFY event, you can set the **“sip xml notify event”** parameter in the configuration files. If the content is missing in the SIP NOTIFY message received by the BluStar 8000i, the BluStar 8000i automatically uses the value you specify for the **“action uri xml sip notify”** parameter.

Use the following procedure to configure the XML SIP NOTIFY events:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [XML SIP Notify Settings](#) on page A-80.

Configurable DNS Queries

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy to remember identifier for an Internet address.

The lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority within a database of records. There is usually a DNS server within close proximity to your geographic location that maps the domain names in your Internet requests or forwards them to other servers in the Internet.

The BluStar 8000i may be configured to issue requests for DNS records using one of three methods. In the first method, the BluStar 8000i issues requests for **“A”** records from the DNS server. In the second method, the BluStar 8000i issues requests for **“SRV”** records from the DNS server. In the third method, the BluStar 8000i issues requests for **NAPTR** records from the DNS server. However, the BluStar 8000i does not use the **NAPTR** record to determine whether to use a secure or unsecure communication path (see the following table for a description of each method).

When the BluStar 8000i accesses the IP network, it issues a DNS lookup request to find the IP address and port and then waits for a response from the DNS service that provides the IP address and port.

Note:

Whether or not the BluStar 8000i will operate/communicate in a secure or unsecure mode is **ONLY** determined by the pre-provisioning of the BluStar 8000i (i.e. the .cfg file).

You can configure the BluStar 8000i to use any one of these methods by entering the applicable value in the configuration files:

Configuration File Value	DNS Server Method Used	Description
0	A only	The BluStar 8000i issues requests for " A " (Host IP Address) records from the DNS server to get the IP address, and uses the default port number of 5060.
1	SRV & A	The BluStar 8000i issues requests for " SRV " (Service Location Record) records from the DNS server to get the port number. Most often, the IP address is included in the response from the DNS server to avoid extra queries. If there is no IP address returned in the response, the BluStar 8000i sends out the request for " A " records from the DNS server to find the IP address.
2	NAPTR & SRV & A	<p>First, the BluStar 8000i sends "NAPTR" (Naming Authority Pointer) lookup to get the "SRV" pointer and service type. For example, if Global SIP transport protocol on the BluStar 8000i is "UDP", and Proxy server on the BluStar 8000i is "test.aastra.com", then:</p> <ol style="list-style-type: none"> 1. If the NAPTR record is returned empty, the BluStar 8000i will use the default value "_sip_udp.test.aastra.com" for the "SRV" lookup. 2. If the NAPTR record is returned "test.aastra.com SIP+D2U_sip_udp.abc.aastra.com", the BluStar 8000i will use "_sip_udp.abc.aastra.com" for the "SRV" lookup. 3. If the NAPTR record is returned "test.aastra.com SIP+D2T_sip_tcp.test.aastra.com", where the service type TCP mismatches the phone configured transport protocol "UDP", the BluStar 8000i will ignore this value and use the default value "_sip_udp.test.aastra.com" for the "SRV" lookup. <p>Note: The BluStar 8000i does not use the service type sent by the NAPTR response to switch its transport protocol, nor does it use the NAPTR response to determine whether to use a secure or unsecure communication path. The BluStar 8000i will always use a global sip protocol that is configured on the BluStar 8000i via configuration files.</p> <p>After performing NAPTR, the phone sends "SRV" lookup to get the IP address and port number. If there is no IP address in the "SRV" response, then it sends out an "A" lookup to get it.</p>

Note:

On the phone side, if you configure the phone with a Fully- Qualified Domain Name (FQDN) proxy and specified port, the phone always sends "**A only**" lookups to find the Host IP Address of the proxy.

Configuring the DNS Query Method

You can configure the DNS query method for the BluStar 8000i to use for performing DNS lookups using the "**sip dns query type**" parameter in the configuration files.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [DNS Query Setting on page A-81](#).

Ignore Out of Sequence Errors

An administrator can configure the BluStar 8000i via the "**sip accept out of order requests**" parameter to ignore CSeq number errors on all SIP dialogs on the BluStar 8000i. When this parameter is enabled, the BluStar 8000i no longer verifies that the sequence numbers increase for each message within a dialog, and does not report a "CSeq Out of Order" error if they do not increase.

Enabling/Disabling “Out of Order SIP Requests”

Use the following procedure to enable/disable out of order SIP requests:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Ignore Out of Order SIP Requests](#) on page A-82.

Switching Between Early Media and Local Ringing

Upon receiving a 180 response, the BluStar 8000i generates a local ring tone unless it is receiving an early media flow.

Configurable “Allow” and “Allow-Event” Optional Headers

On the BluStar 8000i, an administrator can enable or disable whether or not the optional “Allow” and “Allow-Events” headers are included in the NOTIFY message from the BluStar 8000i. SIP NOTIFY messages from the BluStar 8000i may contain optional headers called “Allow” and “Allow-events”. If the NOTIFY message contains these headers, the UDP packet returned by the server may be too large and may fragment the packet.

To prevent the fragmenting of the UDP packet, the “Allow” and “Allow-events” headers may be removed using the parameter, **“sip notify opt headers”**. If this parameter is set to “0” (disabled), the optional headers are not included in the SIP NOTIFY message, which reduces the size of the packet returned by the server, and prevents fragmentation of the packet.

The value set for this parameter specifies whether or not to include the optional headers in the SIP NOTIFY message from the BluStar 8000i. An administrator can enable/disable the optional “Allow” and “Allow-Event” headers using the **“sip notify opt headers”** parameter in the configuration files.

Enabling/Disabling Optional “Allow” and “Allow-Event” Headers

Use the following procedure to enable/disable “Allow” and “Allow-Event” headers:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Optional “Allow” and “Allow-Event” Headers](#) on page A-82.

Configurable SIP P-Asserted Identity (PAI)

The BluStar 8000i support a private extension to SIP for Asserted Identity within trusted networks (as defined in RFC 3325). This feature allows a network of trusted SIP servers to assert the identity of authenticated users, and verify that BluStar 8000i messages originate from a Trusted Identity. Upon receiving a message from a caller in the Trusted Network, the BluStar 8000i reads the contents of the P-Asserted-Identity (PAI) header field and displays it on the BluStar 8000i UI. The BluStar 8000i provide the ability for the administrator to enable or disable the display of PAI information on the BluStar 8000i using the **“sip pai”** parameter in the configuration files.

Enabling/Disabling P-Asserted Identity (PAI)

Use the following procedure to enable/disable PAI:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [P-Asserted Identity \(PAI\)](#) on page A-82.

Configurable Compact SIP Header

The BluStar 8000i provide a feature that allows an administrator to shorten the length of a SIP packet by using the compact form. This feature is in accordance with Compact SIP Headers defined in RFC 3261.

For example, the following SIP header is the long format:

```
Via: SIP/2.0/UDP
10.50.91.2:5060;branch=z9hG4bK571ebe0c;rport=5060;received=10.50.91.2
From: "Unknown" <sip:Unknown@10.50.91.2>;tag=as19d00fc8
To: <sip:1106@10.50.110.54:5060;transport=udp>;tag=916699998
Call-Id: 73cad5456806f3a7768d17e8617279d7@10.50.91.2
CSeq: 102 OPTIONS
```

The following SIP header is equivalent to the above SIP header, however uses the short (compact) format instead:

```
v: SIP/2.0/UDP
10.50.91.2:5060;branch=z9hG4bK571ebe0c;rport=5060;received=10.50.91.2
f: "Unknown" <sip:Unknown@10.50.91.2>;tag=as19d00fc8
t: <sip:1106@10.50.110.54:5060;transport=udp>;tag=916699998
i: 73cad5456806f3a7768d17e8617279d7@10.50.91.2
CSeq: 102 OPTIONS
```

By default, the BluStar 8000i uses the long format. However, an administrator can provision the short (compact) format using the **"sip compact headers"** parameter in the configuration files.

Enabling/Disabling the Compact SIP Headers Feature

Use the following procedure to enable/disable the Compact SIP Header in the SIP packet:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Compact SIP Header](#) on page A-83.

Configurable Dial Plan Terminator

The BluStar 8000i provides a feature that allows an administrator to configure whether or not pressing the hash/pound (i.e. "#") key while performing an outgoing call on an open line acts as a dial plan terminator (i.e. dials out the call immediately). By default, the hash/pound key is configured as a dial plan terminator; however, an administrator can change the behavior using the "**sip dial plan terminator**" parameter so that pressing the hash/pound key is sent as %23 instead.

Configuring the Dial Plan Terminator Feature

Use the following procedure to configure the dial plan terminator feature:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Dial Plan Terminator](#) on [page A-83](#).

Chapter 6

Troubleshooting

The chapter describes information available to an administrator for troubleshooting purposes. It also includes answers to questions you may have while using the BluStar 8000i in SIP Call Server mode.

BluStar 8000i Status

In the app menu on the BluStar 8000i UI, you can find information about the terminal by selecting the **about** or **status** apps.

About

The about app provides software, hardware, copyright, restrictions, and limited rights information for the BluStar 8000i. You will see the following information on the about screen:

- Software
- Hardware
- Serial number
- MAC address
- IP address
- Legal information



Status

When the BluStar 8000i terminal is idle, the status app displays current operating status and version information.

Network Info

Displays network address and link status for the terminal's network connection. If ATM is connected, network info provides a link to view the UNI configuration settings.

Detailed Media Info

- Audio Details
 - Displays details about the audio configuration and audio packet statistics
 - Displays transmit and receive statistics for the terminal's audio traffic
- Video Details
 - Displays details about the self view and main window statistics
 - Displays transmit and receive statistics for the terminal's video traffic
 - Displays camera status information
 - Displays video codec status information
 - Displays details about the video display

10/100/1000M Gigabit Ethernet Switch Controller

Displays information on link status information.

System Temperature and Voltage Sensors

Displays the current temperature and voltage levels of the terminal systems.

Disk Info

Displays disk and memory usage information.

VAV Driver Info

Displays information about the BluStar 8000i Encoder DSP driver.

Memory/System Info

Displays details about the system processes, terminal up time, CPU load, and memory usage.

Server Configuration Files

Displays which server configuration files (i.e. security.tuz, aastra.cfg/tuz, <model>.cfg/tuz, and <mac>.cfg/tuz) and licences have been downloaded successfully at boot up. Transfer failures of any critical files (e.g. aastra.cfg) are indicated in bold red.

User Configuration Files

Displays which user configuration files (i.e. security.tuz, <user>.cfg/tuz, <user>_local.cfg/tuz) have been downloaded successfully at boot up.

Configuration Info

Contains links to terminal configuration (aastra.cfg, <model>.cfg, and <mac>.cfg) information and user configuration (<user>.cfg) files.

Licensed Features

Displays details about the specific licenses installed for the BluStar 8000i terminal.

Graphic Status Page

During calls on the BluStar 8000i, administrators can select the status app on the respective terminal and a graphic status page will be displayed detailing information regarding the following items:

- Transmit rate
- Receive rate
- Packet loss
- Queue statistics

Data is collected and the graphs are refreshed every two seconds.

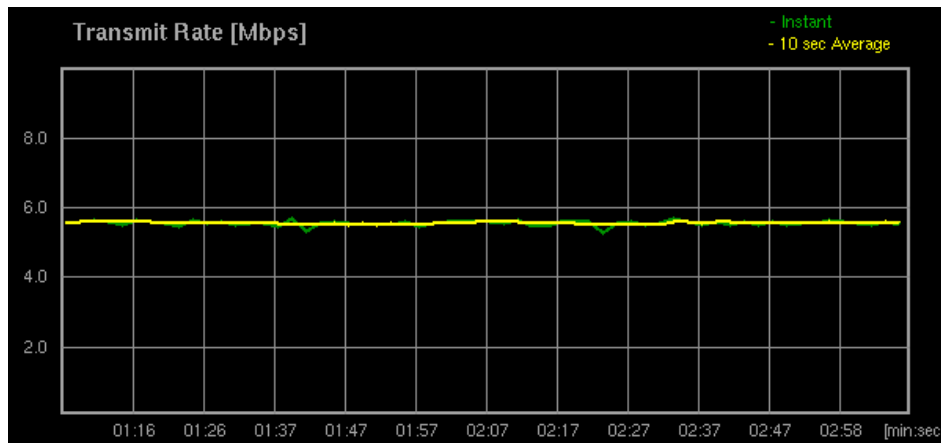
Note:

At any time, touching **done** will bring back the initial call screen.



Transmit Rate

The top-left graph displays the transmit rate in Mbps. The graph encompasses a plot for instantaneous values as well as a plot representing 10 second averages. The plots reflect the combined rate of all users connected to the call.



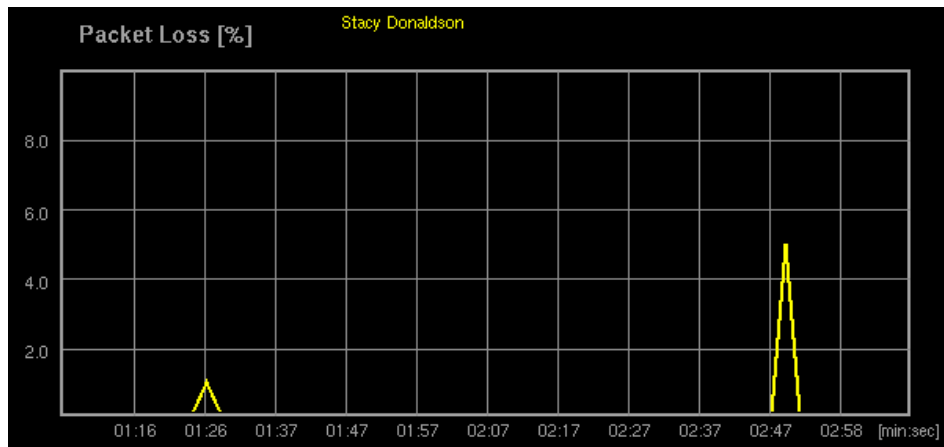
Receive Rate

The bottom-left graph displays the receive rate in Mbps. The graph encompasses a plot for instantaneous values as well as a plot representing 10 second averages. The plots reflect the combined rate of all users connected to the call.



Packet Loss

The top-right graph displays packet loss in %. The plotted values reflect the packet loss encountered by respective users participating in the call.



Queue Statistics

The bottom-right graph displays the following queue statistics:

- Jitter buffer size for the channel
- Number of out-of-order packets for the channel
- Number of dropped packets for the channel



Note:

Dropped packets do not affect the packet loss statistics as the packets are intentionally dropped after they are received.

Details

Touching **details** while on the graphic status page will display the information listed in the idle status page as well as information related to the following additional categories:

- Network stats - Audio
 - Displays details about the audio transmit and receive channels including packet statistics, bitrate data, and packet/stream type.
- Network stats - Video
 - Displays details about the video transmit and receive channels including packet statistics, bitrate data, and packet/stream type.

For more information on the idle status page, see [Status](#) on [page 6-1](#).

On-Screen Connection Quality Alarms

Poor Network Performance

When poor network performance is experienced during a call on the BluStar 8000i, the following alert is displayed on screen:

Poor Network Performance - Call Quality is Degrading

Touching the on-screen alert will automatically display the graphic status page. For more information on the graphic status page, see [Graphic Status Page](#) on [page 6-3](#).

Very Poor Network Performance

When very poor network performance is experienced during a call on the BluStar 8000i, the following alert is displayed on screen:

Network Performance Very Poor...BluStar is auto adapting

Touching the on-screen alert will automatically display the graphic status page. For more information on the graphic status page, see [Graphic Status Page](#) on [page 6-3](#).

Configuration parameters are available allowing administrators to set the thresholds of how much packet loss occurs before displaying the above alerts.

To Configure On-Screen Connection Quality Alarms

Use the following procedure to configure the on-screen connection quality alarms:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [On-Screen Connection Quality Alarms](#) on [page A-84](#).

Syslog Settings

Syslog is a administration logging standard, whereby messages can be logged by facility and severity. Administrators can access and configure Syslog features on the BluStar 8000i. Syslog parameters have been implemented and can be configured for the following log-related items:

- Syslog location
- System-wide logging
- SIP stack logging
- Debug logging

Syslog Location

Using the configuration files, administrators can specify the save location of the log files used for troubleshooting purposes.

The following parameters can be edited to configure the Syslog location settings:

Parameters in Configuration Files	Description
log server ip	Specifies the log server IP address for which to save system log files for troubleshooting purposes. For example, log server ip: 192.168.3.2
log server port	Specifies the log server IP port to use to save log files for troubleshooting purposes. For example, log server port: 514

To Configure Syslog Location Settings:

Use the following procedure to configure the Syslog location settings.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Syslog Settings on page A-85](#).

System-Wide Logging

The following parameters can be edited to configure the system-wide log settings. These parameters must be prefaced by the term “BluStar Settings:”.

Parameters in Configuration Files	Description
LogLevel	Sets the baseline log level for all of the modules. Individual modules will use the higher of this parameter of their own specific setting. For example, BluStar Settings: LogLevel=2
WriteToFlag	A mask that controls the data path(s) for the logging data. For example, BluStar Settings: WriteToFlag=0

To Configure System-Wide Log Settings:

Use the following procedure to configure the system-wide log settings:



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Syslog Settings on page A-85](#).

SIP Stack Logging

The following parameters can be edited to configure the SIP stack log settings. These parameters must be prefaced by the term “BluStar Settings:”

Parameters in Configuration Files	Description
VSipServer_LogLevel	Sets the SIP stack log level. For example, BluStar Settings: VSipServer_LogLevel=5
VSipServer_WriteToFlag	A mask that controls the data path(s) for the SIP stack logging data. For example, BluStar Settings: VSipServer_WriteToFlag=1

To Configure the SIP Stack Log Settings:

Use the following procedure to configure the SIP stack log settings.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Syslog Settings](#) on page A-85.

Debug Logging

The following parameters can be edited to configure the debug log settings. These parameters must be prefaced by the term “BluStar Settings:”

Parameters in Configuration Files	Description
DBG_Modules	Allows for enhanced severity filtering of log calls for specific debug modules. For example, BluStar Settings: DBG_Modules=SESN, CALL
DBG_LogLevel	Sets the debug log level. Note: The debug log level must be less than or equal to the system-wide log level for the debug module logging to output. For example, BluStar Settings: DBG_LogLevel=1
DBG_WriteToFlag	A mask that controls the data path(s) for the debug logging data. For example, BluStar Settings: DBG_WriteToFlag=1

To Configure the Debug Log Settings:

Use the following procedure to configure the debug log settings.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Syslog Settings](#) on page A-85.

Troubleshooting Solutions

How do I restart the BluStar?

You can restart the BluStar 8000i from the app menu. From the log off screen, users have the option to do the following:

- log off
- log off and restart
- log off and shut down
- safe shutdown for unit relocation
- cancel

To Log Off:

1. Touch the **app menu**.
2. Touch the **log off** button.
3. Touch either:
 - **log off**
 - **log off and restart**
 - **log off and shut down**
 - **safe shutdown for unit relocation**

How do I set the BluStar to factory default?

You can set the BluStar 8000i to its factory default setting on the BluStar 8000i UI. Factory default settings are the settings that reside on the BluStar 8000i after it has left the factory. Factory default settings on the BluStar 8000i set factory defaults for all of the settings in the aastra.cfg, <model>.cfg, and <mac>.cfg files.

Note:

Resetting the terminal to factory default will not change the <user>.cfg.

To Reset to Factory Defaults:

1. Touch **reset to factory defaults** button.
The following message appears: "Do you really want to log off and reset to factory defaults?"
2. Press either **Reset** or **Cancel**.

How can I send comments or report a bug concerning my BluStar?

A feedback application is available in the app menu that you can use to send comments and/or report issues directly to Aastra Telecom from your BluStar 8000i terminal. The feedback application can be enabled or disabled in the configuration files.

To Send Comments or Report Issues Using the Feedback Application:

1. Touch the **app menu** button
OR
the **hot** key.
The app menu button is outlined in green, indicating that it is opened.
2. Touch the **feedback** button.

3. Touch the **feedback type** field and select the general category of feedback you wish to send.
Note:
If the applicable general category is not listed, select **other**.
4. Touch the **your email** field and enter your email address by using the on-screen keyboard.
Note:
Including your email address is optional.
5. Touch the **comment/details** field and enter any comments or issue details by using the on-screen keyboard. If you are reporting an issue, please state precisely all relevant information pertaining to the issue.
Note:
At any time, touching the **reset form** button will discard all changes and revert the form back to its original state.
6. Touch **submit form** if no further changes are needed.
7. Touch **done** to return to your home screen.

To Configure the Feedback Application:

Use the following procedure to configure the feedback application.



Configuration Files

For the specific parameter(s) you can set in the configuration files, see Appendix A, the section, [Feedback Application Settings](#) on [page A-90](#).

Appendix A

Parameters

Introduction

This appendix describes the parameters you can set in the configuration files for the BluStar 8000i. The configuration files include `aastra.cfg`, `<model>`, `<mac.cfg>`, and `<user>.cfg`.

Topics

This appendix covers the following topics:

Topic	Page
Setting Parameters in Configuration Files	page A-3
Operational, Basic Parameters	page A-4
Network Settings	page A-4
ToS/QoS/Diffserv QoS Parameters	page A-8
Virtual Local Area Network (VLAN) Settings	page A-8
DHCP Option Settings	page A-10
Configuration Server Settings	page A-11
Rport Setting	page A-20
SIP Settings	page A-20
Advanced SIP Settings	page A-25
Directory Settings	page A-28
Call History Settings	page A-30
Missed Calls Indicator Settings	page A-30
Basic LDAP Settings	page A-30
Advanced LDAP Settings	page A-32
Microsoft Exchange Contact Settings	page A-44
LDAP Directory/Exchange Contacts Update Interval	page A-47
User Settings	page A-49
Power Saving Schedule Settings	page A-49
Terminal Security Settings	page A-56
Screen Settings	page A-58
Locale Settings	page A-60
Audio/Video Settings	page A-63
Call Forward Settings	page A-65
Incoming Intercom Call Auto-Answer Settings	page A-68
Voicemail Settings	page A-68

Topic	Page
Video Voicemail Client Integration Settings	page A-69
Emergency Dial Plan Settings	page A-70
Picture ID Feature	page A-75
BLF List URI Settings	page A-75
BLF Subscription Period Settings	page A-76
Directed Call Pickup	page A-76
XML Settings	page A-77
Advanced Operational Parameters	page A-78
Update Caller ID Setting	page A-78
Blind Transfer Setting	page A-78
User-Agent Settings	page A-78
Inactive Video Stream Settings	page A-79
Blacklist Duration Setting	page A-79
Whitelist Proxy Setting	page A-79
XML SIP Notify Settings	page A-80
DNS Query Setting	page A-81
Ignore Out of Order SIP Requests	page A-82
Optional “Allow” and “Allow-Event” Headers	page A-82
P-Asserted Identity (PAI)	page A-82
Compact SIP Header	page A-83
Dial Plan Terminator	page A-83
Troubleshooting Parameters	page A-84
On-Screen Connection Quality Alarms	page A-84
Syslog Settings	page A-85
Feedback Application Settings	page A-90

Setting Parameters in Configuration Files

You can set specific configuration parameters in the configuration files for configuring a BluStar 8000i. The **aastra.cfg**, **<model>.cfg**, **<mac>.cfg**, and **<user>.cfg** files are stored on the server.

Note:

The **<user>_local.cfg** is also stored on the server but the file must never be edited manually. All user parameters that need to be configured should be defined and edited in the **<user>.cfg** file only.

The **aastra.cfg** file contains configuration information about all BluStar and/or all 9000i and 6700i series IP SIP phone devices.

The **<model>.cfg** file contains model specific information.

The **<mac>.cfg** file stores configuration settings specific to the BluStar with that MAC address, and has the parameter **"update url"** that downloads software onto the BluStar 8000i.

The **<user>.cfg** file contains read-only server-related user configuration information that is not configurable through the BluStar 8000i terminal.

Notes:

- The majority of configuration parameters that you enter in the configuration files are **NOT** case sensitive, however language values (e.g. French) **ARE** case sensitive.
- All URL parameters containing special characters found within applicable configuration files must be URL-encoded. Examples of applicable special characters can be found in the table in [On-Screen Keyboard](#) on [page 1-15](#). Please refer to RFC3986 for further details.

Reference

For information about configuration file precedence, see [Configuration Precedence](#) on [page 2-2](#).

Operational, Basic Parameters

The following sections provide the configuration parameters you can configure on the BluStar 8000i. Each parameter table includes the name of the parameter, a description, the format, default value, range, and example. The table also provides the method for which the parameters can be configured (e.g. aastra.cfg, <model>.cfg, <mac>.cfg, or <user>.cfg).

Network Settings

Parameter – <i>dhcp</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables DHCP. Enabling DHCP populates the required network information. The DHCP server serves the network information that the BluStar 8000i requires. If the BluStar 8000i is unable to get any required information, then you must enter it manually. DHCP populates the following network information: IP Address, Subnet Mask, Gateway, Domain Name Servers (DNS), HTTP HTTPS, TFTP, and FTP servers, and Timer Servers.
Format	Integer
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	dhcp: 1

Parameter – <i>ip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	This parameter assigns a static IP address to the BluStar 8000i. For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
Format	IP address
Default Value	0.0.0.0
Range	NA
Example	ip: 192.168.0.25

Parameter – <i>subnet mask</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Subnet mask defines the IP address range local to the BluStar 8000i. For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
Format	IP address
Default Value	255.255.255.0
Range	NA
Example	subnet mask: 255.255.255.224

Parameter – <i>default gateway</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The IP address of the network's gateway or default router IP address. For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
Format	IP address
Default Value	1.0.0.1
Range	NA
Example	default gateway: 192.168.0.1

Parameter – <i>dns1</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Primary domain name server IP address. For any of the IP address settings on the BluStar 8000i, a domain name value can be entered instead of an IP address. With the help of the domain name servers the domain names for such parameters can then be resolved to their corresponding IP addresses. For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
Format	IP address
Default Value	0.0.0.0
Range	NA
Example	dns1: 192.168.0.5

Parameter – <i>dns2</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	A service that translates domain names into IP addresses. To assign static DNS addresses, disable DHCP. For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
Format	IP address
Default Value	0.0.0.0
Range	NA
Example	dns2: 192.168.0.6

Parameter – <i>ethernet port 0</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The send (TX) and receive (RX) method to use on Ethernet port 0 to transmit and receive data over the LAN.
Format	Integer
Default Value	0
Range	0-4 0 (auto-negotiate) 1 (full-duplex, 10Mbps) 2 (full-duplex, 100Mbps) 3 (half-duplex, 10Mbps) 4 (half-duplex, 100Mbps)
Example	ethernet port 0: 3

Parameter – <i>time server disabled</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables the time server. This parameter affects the “ time server1 ”, “ time server2 ”, and “ time server3 ” parameters. Setting this parameter to ‘0’ allows the use of the configured Time Server(s). Setting this parameter to ‘1’ prevents the use of the configured Time Server(s). For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
Format	Integer
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	time server disabled: 0

Parameter – <i>time server1</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The primary time server's IP address or qualified domain name. If the time server is enabled, the value for “ time server1 ” will be used to request the time from. For DHCP to automatically populate this parameter, your DHCP server must support Option 66.
Format	IP address or qualified domain name
Default Value	0.0.0.0
Range	NA
Example	time server1: 192.168.0.5

Parameter – <i>time server2</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The secondary time server's IP address or qualified domain name. If the time server is enabled and the primary time server is not configured or cannot be accessed, the value for “ time server2 ” will be used to request the time from.
Format	IP address or qualified domain name
Default Value	0.0.0.0
Range	NA
Example	time server2: 192.168.0.5

Parameter – <i>time server3</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The tertiary time server's IP address or qualified domain name. If the time server is enabled and the primary and secondary time servers are not configured or cannot be accessed, the value for “ time server3 ” will be used to request the time from.
Format	IP address or qualified domain name
Default Value	0.0.0.0
Range	NA
Example	time server3: 192.168.0.5

ToS/QoS/Diffserv QoS Parameters

Parameter – <i>tos sip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The Differentiated Services Code Point (DSCP) for SIP packets.
Format	Integer
Default Value	46
Range	0-63
Example	tos sip: 3

Parameter – <i>tos rtp</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The Differentiated Services Code Point (DSCP) for audio RTP packets.
Format	Integer
Default Value	46
Range	0-63
Example	tos rtp: 2

Parameter – <i>tos rtp video</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The Differentiated Services Code Point (DSCP) for video RTP packets.
Format	Integer
Default Value	46
Range	0-63
Example	tos rtp video: 4

Virtual Local Area Network (VLAN) Settings

Global Parameters

Parameter – <i>tagging enabled</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables VLAN on the BluStar 8000i. This is a global setting.
Format	Boolean
Default Value	0 (Disabled)
Range	0 (Disabled) 1 (Enabled)
Example	tagging enabled: 1

LAN Port (Ethernet Port 0) Parameters

Parameter – <i>vlan id</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 0 (LAN port).
Format	Integer
Default Value	1
Range	1 to 4094
Example	vlan id: 300

Parameter – <i>qos eth port 0 priority</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the priority value used for all traffic (e.g. SIP, RTP, etc.) on the physical Ethernet Port 0.
Format	Integer
Default Value	5
Range	0 to 7
Example	qos eth port 0 priority: 2

PC Port (Ethernet Port 1) Parameters

Parameter – <i>vlan id port 1</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Allows you to configure a VLAN ID that associates with the physical Ethernet Port 1 (PC port).
Format	Integer
Default Value	1
Range	1 to 4094
Example	vlan id port 1: 3

Parameter – <i>qos eth port 1 priority</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the priority value used for passing VLAN packets through to a PC via Port 1.
Format	Integer
Default Value	0
Range	0 to 7
Example	qos eth port 1 priority: 3

DHCP Option Settings

Option 12

Parameter– <i>hostname</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the hostname DHCP Option 12 that the BluStar 8000i sends with the DHCP Request packet. If you change this parameter, you must restart the BluStar 8000i for the change to take affect.
Format	String
Default Value	[<model><MAC IP Address>]
Range	Up to 64 alpha-numeric characters The value for this parameter can also be a fully qualified domain name.
Example	hostname: aastra4

Option 77

Parameter– <i>dhcp userclass</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the User Class DHCP Option 77 that the BluStar 8000i sends to the configuration server with the DHCP Request packet. If you specify a value for this parameter, you must restart your BluStar 8000i for the change to take affect. Any change in its value during start-up results in an automatic reboot.
Format	String
Default Value	""
Range	Up to 64 alpha-numeric characters
Example	dhcp userclass: admin

Options 159 and 160 - DHCP Option Override

Parameter – <i>dhcp config option override</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The value specified for this parameter overrides the precedence order for determining a configuration server. Note: You must restart the BluStar for this parameter to take affect.
Format	Integer
Default Value	0 (any - no override - uses normal precedence order of 43, 160, 159, 66)
Range	-1 (disabled - ignores all DHCP configuration options (43, 66, 159, 160)) 0 (any) 43 66 159 160
Example	dhcp config option override: 66

Configuration Server Settings

Parameter – <i>pbx mode</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	This parameter specifies the BluStar 8000i mode. Note: If configuration server details are being set by the DHCP server, ensure that the locked parameter “ !pbx mode: 1 ” is added to the aastra.cfg file for SIP Call Server mode. As the default server type is locally set to BluStar Application Server on the BluStar 8000i and the local terminal settings take precedence over the configuration files, failure to lock the “ pbx mode ” parameter may cause the BluStar 8000i to boot into BluStar Application Server mode upon a restart.
Format	Integer
Default Value	0 (BAS mode)
Range	0-1 0 (BAS mode) 1 (SIP Call Server mode)
Example	!pbx mode: 1

Parameter – <i>download protocol</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Protocol to use for downloading the configuration files to the BluStar 8000i.
Format	Text
Default Value	FTP
Range	TFTP FTP HTTP HTTPS
Example	download protocol: http

Parameter – <i>download timeout</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the overall timeout (in seconds) for downloading the configuration files (aastra.cfg, <model>.cfg, and <mac>.cfg).
Format	Integer
Default Value	30 (seconds)
Range	Minimum value is 10 seconds.
Example	download timeout: 40

Parameter – <i>download connect timeout</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Complements the “download timeout” parameter. Whereas the “download timeout” parameter is used to specify the timeout for downloading the configuration files, the “download connect timeout” parameter specifies the amount of time allowed (in seconds) for the BluStar 8000i to connect to the configuration server.
Format	Integer
Default Value	15 (seconds)
Range	Minimum value is 5 seconds.
Example	download connect timeout: 20

Parameter – <i>update url</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The url to upgrade the BluStar 8000i software. Note: The software upgrade process will be initiated on the first reboot after the parameter has been modified.
Format	url
Default Value	NA
Range	File transfer protocol can be FTP, HTTP, or HTTPS
Example	update url: ftp://10.55.102.56/aastracfg

Parameter – <i>user config url</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The url to load the user configuration files.
Format	url
Default Value	NA
Range	File transfer protocol can be TFTP, FTP, HTTP, or HTTPS Note: The “user config url” parameter supports tftp, ftp, http, https, however only ftp, http, and https can be authenticated.
Example	user config url: http://10.55.102.56/aastracfg/usercfg

Parameter – <i>enable user configuration server redirection</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used to enable HTTP(S) redirection when downloading the user.cfg and downloading/uploading the user_local.cfg files in such cases where the files are statically configured (in the aastra.cfg, <mac>.cfg, or <model>.cfg files) to a single location, but the user configuration files are in fact located on the SIP call server node hosting the subscription. If the parameter is disabled in such cases, the BluStar 8000i cannot properly retrieve the user configuration files.
Format	Boolean
Default Value	0
Range	0-1 0 (disabled) 1 (enabled)
Example	enable user configuration server redirection: 1

Parameter – <i>telephony integration url</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The url (http or https) the BluStar 8000i calls to perform SIP Call Server integration. This is done during the login sequence and later to activate/deactivate server side feature integration such as DND, Call Forward, etc.
Format	String
Default Value	NA
Range	NA
Example	telephony integration url: http://myserver.com/integration.php

Parameter – <i>telephony integration use login credentials</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	By default BluStar 8000i uses the SIP credentials to authenticate (digest method) to the SIP Call Server integration server. Enabling this configuration parameter makes BluStar 8000i use the user login/password instead.
Format	Boolean
Default Value	0
Range	0-1 0 (disabled) 1 (enabled)
Example	telephony integration use login credentials: 1

Parameter – <i>telephony integration needs sip registration</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used by the telephony integration API to indicate to the software if SIP registration is needed before sending a user command via the API. When enabled, the BluStar 8000i checks the extension registration status before sending an API command. If the extension is not registered, an error message is displayed.
Format	Boolean
Default Value	0
Range	0-1 0 (disabled) 1 (enabled)
Example	telephony integration needs sip registration: 1

Parameter – <i>tftp server</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>The TFTP server's IP address. If DHCP is enabled and the DHCP server provides the information, this field is automatically populated. Use this parameter to change the IP address or domain name of the TFTP server. This will become effective after this configuration file has been downloaded into the BluStar 8000i.</p> <p>Note: For DHCP to automatically populate this parameter, your DHCP server must support Option 66.</p>
Format	IP address or qualified domain name
Default Value	0.0.0.0
Range	NA
Example	tftp server: 192.168.0.130

Parameter – <i>tftp port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Specifies the path name for which the configuration files reside on the TFTP server for downloading to the BluStar 8000i.</p> <p>Note: Enter the path name in the form folderX\folderX. For example, blustar8000i\configfiles.</p>
Format	String
Default Value	NA
Range	Up to 64 alphanumeric characters
Example	tftp path: configs\tftp

Parameter – <i>ftp server</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>The FTP server's IP address or network host name. This will become effective after this configuration file has been downloaded into the BluStar 8000i.</p> <p>Optional: You can also assign a user name and password for access to the FTP server. See the following parameters for setting user name and password.</p> <p>Note: For DHCP to automatically populate this parameter, your DHCP server must support Option 66.</p>
Format	IP address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	NA
Example	ftp server: 192.168.0.131

Parameter – <i>ftp path</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies a path name for which the configuration files reside on an FTP server for downloading to the BluStar 8000i. Note: Enter the path name in the form <i>folderX\folderX\folderX</i> . For example, BluStar8000i\BluStarconfigfiles.
Format	String
Default Value	NA
Range	Up to 64 alphanumeric characters
Example	ftp path: configs\ftp

Parameter – <i>ftp username</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The user name to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the BluStar 8000i. Note: The BluStar 8000i supports user names containing dots (".").
Format	Text
Default Value	NA
Range	Up to 63 alphanumeric characters
Example	ftp username: aastraconfig

Parameter – <i>ftp password</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The password to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the BluStar 8000i.
Format	Text
Default Value	NA
Range	Up to 63 alphanumeric characters
Example	ftp password: 1234

Parameter – <i>http server</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>The HTTP server's IP address. This will become effective after this configuration file has been downloaded into the BluStar 8000i.</p> <p>Optional: You can also assign an HTTP relative path to the HTTP server. See the next parameter (http path).</p> <p>Note: For DHCP to automatically populate this parameter, your DHCP server must support Option 66.</p>
Format	IP address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	NA
Example	http server: 192.168.0.132

Parameter – <i>http path</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>The HTTP path name to enter.</p> <p>If the BluStar 8000i's configuration and firmware files are located in a sub-directory beneath the server's HTTP root directory, the relative path to that sub-directory should be entered in this field.</p>
Format	dir/dir/dir
Default Value	NA
Range	Up to 63 alphanumeric characters
Example	http path: blustar/1

Parameter – <i>http port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Specifies the HTTP port that the server uses to load the configuration to the BluStar 8000i over HTTP.</p> <p>Note: For DHCP to automatically populate this parameter, your DHCP server must support Option 66.</p>
Format	Integer
Default Value	80
Range	1 through 65535
Example	http port: 1025

Parameter – <i>https server</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>The HTTPS server's IP address. This will become effective after this configuration file has been downloaded into the BluStar 8000i.</p> <p>Optional: You can also assign an HTTPS relative path to the HTTPS server. See the next parameter (https path).</p> <p>Note: For DHCP to automatically populate this parameter, your DHCP server must support Option 66.</p>
Format	IP address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	NA
Example	https server: 192.168.0.143

Parameter – <i>https path</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>The HTTPS path name to enter.</p> <p>If the BluStar 8000i's configuration and firmware files are located in a sub-directory beneath the server's HTTPS root directory, the relative path to that sub-directory should be entered in this field.</p>
Format	dir/dir/dir
Default Value	NA
Range	Up to 63 alphanumeric characters
Example	https path: blustar/1

Parameter – <i>https port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Specifies the HTTPS port that the server uses to load the configuration to the BluStar 8000i over HTTPS.</p> <p>Note: For DHCP to automatically populate this parameter, your DHCP server must support Option 66.</p>
Format	Integer
Default Value	443
Range	1 through 65535
Example	https port: 1025

Parameter – <i>auto resync mode</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Determines whether the configuration server automatically updates the configuration files or disables automatic updates. This parameter works with TFTP, FTP, HTTP and HTTPS servers.</p> <p>Valid values are: None (0) - Disable auto-resync Configuration Files (1) - Updates the configuration files on the BluStar 8000i automatically at the specified time if the files on the server have changed.</p> <p>Notes:</p> <ul style="list-style-type: none"> Any changes made using the BluStar 8000i are not overwritten by an auto-resync update. Auto-resync affects the configuration files only. The resync time is based on the local time of the BluStar 8000i. If the BluStar 8000i is in use (not idle) at the time of the resync check, the reboot occurs when the BluStar 8000i becomes idle. The automatic update feature works with both encrypted and plain text configuration files.
Format	Integer
Default Value	0
Range	0-1 0 (none) 1 (configuration files only)
Example	auto resync mode: 1

Parameter – <i>auto resync time</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Sets the time of day in a 24-hour period for the BluStar 8000i to be automatically updated. This parameter works with TFTP, FTP, HTTP and HTTPS servers.</p> <p>Notes:</p> <ul style="list-style-type: none"> The resync time is based on the local time of the BluStar 8000i. The value of 00:00 is 12:00 A.M. When entering a value for this parameter using the configuration files, the value can be entered using minute values from 00 to 59 (for example, the auto resync time can be entered as 02:56). Auto-Resync adds up to 15 minutes random time to the configured time. For example, if the auto resync time parameter is set to 02:00, the event takes place any time between 02:00 and 02:15. When the language on the BluStar 8000i is set to French or Spanish, you must enter the time in the format "00h00" (configuration files only).
Format	String hh:mm 00h00 (for French and Spanish configuration files)
Default Value	00:00
Range	00:00 to 23:59
Example	auto resync time: 22:30

Parameter – <i>auto resync max delay</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum time, in minutes, the BluStar 8000i waits past the scheduled time before starting a checksync.
Format	Integer
Default Value	0
Range	0-1439
Example	auto resync max delay: 20

Rport Setting

Parameter – <i>sip rport</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	<p>Allows you to enable (1) or disable (0) the use of Rport on the BluStar 8000i.</p> <p>“Rport” in RFC 3581, allows a client to request that the server send the response back to the source IP address and the port from which the request came.</p> <p>Configuring the Rport parameter is recommended for clients behind a Network Address Translation (NAT) or firewall.</p>
Format	Boolean
Default Value	0
Range	0 (disable) 1 (enable)
Example	sip rport: 1

SIP Settings

SIP Authentication Settings

Parameter – <i>sip auth name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used in the user name field of the Authorization header field of the <i>SIP REGISTER</i> request.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip auth name: 5553456

Parameter – <i>sip display name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used in the display name field of the <i>From</i> SIP header field. Some IP PBX systems use this as the caller's ID and some may overwrite this with the string that is set at the PBX system.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip display name: Joe Smith

Parameter – <i>sip screen name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used to display text on the screen of the BluStar 8000i. You may want to set this parameter to display the user's name of the BluStar 8000i.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip screen name: Joe Smith

Parameter – <i>sip screen name 2</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used to display text on a second line on the screen of the BluStar 8000i.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip screen name 2: Lab Phone

Parameter – <i>sip user name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	User name used in the name field of the <i>SIP URI</i> for the BluStar 8000i and for registering the BluStar 8000i at the registrar. Note: The BluStar 8000i support user names containing dots ("").
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip user name: 1010

Parameter – <i>sip password</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The password that will be used to register at the registrar.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip password: 12345

Parameter – <i>sip mode</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Allows you to configure the mode of the line. Applicable values are: Generic - Normal line BroadSoft SCA - Shared Call/Line Appearances (SCA) line for BroadWorks network (call activity can go to more than one BluStar 8000i) BLA - Bridged Line Appearance (BLA) line.
Format	Integer
Default Value	0
Range	0-3 0 - Generic 1 - BroadSoft SCA 2 - (reserved) 3 - BLA
Example	sip mode: 2

Parameter – <i>dash delimiter</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Enables the (-) to visually separate the dial number and to make the number easy to recognize and remember. For example: 5551212: Local phone number with no area code and no dash delimiter 555-1212: Local phone number with no area code and dash delimiter This parameter can be applied in the <user>.cfg file for user specific settings, or in the aastra.cfg or <mac>.cfg files for terminal specific settings.
Format	Boolean
Default Value	0 (No)
Range	0-1 0 (Disabled) 1 (Enabled)
Example	dash delimiter: 1

SIP Network Settings

Parameter – <i>sip proxy ip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The IP address of the SIP proxy server for which the BluStar 8000i uses to send all SIP requests. A SIP proxy is a server that initiates and forwards requests generated by the BluStar 8000i to the targeted user.
Format	IP address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	Up to 64 alphanumeric characters.
Example	sip proxy ip: 192.168.0.101

Parameter – <i>sip proxy port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The proxy server's port number.
Format	Integer
Default Value	0
Range	NA
Example	sip proxy port: 5060

Parameter – <i>sip outbound proxy</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	This is the address of the outbound proxy server. All SIP messages originating from the BluStar 8000i are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here.
Format	IP Address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	NA
Example	sip outbound proxy: 10.42.23.13

Parameter – <i>sip outbound proxy port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The proxy port on the proxy server to which the BluStar 8000i sends all SIP messages.
Format	Integer
Default Value	0
Range	NA
Example	sip outbound proxy port: 5060

Parameter – <i>sip registrar ip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The address of the registrar for which the BluStar 8000i uses to send <i>REGISTER</i> requests. A SIP registrar is a server that maintains the location information of the BluStar 8000i. A value of 0.0.0.0 disables registration. However, the BluStar 8000i is still active and you can dial using the username@ip address of the BluStar 8000i.
Format	IP address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	NA
Example	sip registrar ip: 192.168.0.101

Parameter – <i>sip registrar port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The registrar's port number.
Format	Integer
Default Value	0
Range	NA
Example	sip registrar port: 5060

Parameter – <i>sip registration period</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The requested registration period, in seconds, from the registrar.
Format	Integer
Default Value	0
Range	0 - 2147483647
Example	sip registration period: 3600

Shared Call Appearance (SCA) Call Bridging

Parameter – <i>sip sca bridging</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables/disables SCA bridging on the terminal-side on a global basis. Note: You must restart the terminal after setting a value for this parameter.
Format	Boolean
Default Value	0
Range	0 (disabled) 1 (enabled)
Example	sip sca bridging: 1

Advanced SIP Settings

Parameter – <i>sip explicit mwi subscription</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	If the BluStar 8000i has a message waiting subscription with the Service Provider, a Message Waiting Indicator (MWI) (LED or display icon) tells the user there is a message on the BluStar 8000i.
Format	Boolean
Default Value	0
Range	0-1 0 (disable) 1 (enable)
Example	sip explicit mwi subscription: 1

Parameter – <i>sip explicit mwi subscription period</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The requested duration, in seconds, before the MWI subscription times out. The BluStar 8000i re-subscribes to MWI before the subscription period ends.
Format	Integer
Default Value	86400
Range	30 - 2147483647
Example	sip explicit mwi subscription period: 30

Parameter – <i>sip send mac</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Adds an "Aastra-Mac:" header to the SIP REGISTER messages sent from the BluStar 8000i to the call server, where the value is the MAC address of the BluStar 8000i.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	sip send mac: 1

Parameter – <i>sip out-of-band dtmf</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables out-of-band DTMF. Enabling this parameter forces the BluStar 8000i to use out-of-band DTMF according to RFC2833.
Format	Boolean
Default Value	1
Range	0-1 0 (Inband) 1 (Out-of-band (RFC2833))
Example	sip out-of-band dtmf: 0

Parameter – <i>sip dtmf method</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Sets dual-tone multifrequency (DTMF) method to use on the BluStar 8000i.
Format	Boolean
Default Value	0 (RTP)
Range	0-2 0 (RTP) 1 (SIP info) 2 (both)
Example	sip dtmf method: 1

Parameter – <i>sip session timer</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The time, in seconds, that the BluStar 8000i uses to send periodic re-INVITE requests to keep a session alive. The proxy uses these re-INVITE requests to maintain the status' of the connected sessions. See RFC4028 for details.
Format	Integer
Default Value	0
Range	NA
Example	sip session timer: 30

Parameter – <i>sip T1 timer</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	This timer is a SIP transaction layer timer defined in RFC 3261. Timer 1 is an estimate, in milliseconds, of the round-trip time (RTT).
Format	Integer
Default Value	500
Range	NA
Example	sip T1 timer: 600

Parameter – <i>sip T2 timer</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	This timer is a SIP transaction layer timer defined in RFC 3261. Timer 2 represents the amount of time, in milliseconds, a non-INVITE server transaction takes to respond to a request.
Format	Integer
Default Value	0
Range	NA
Example	sip T2 timer: 8

Parameter – <i>sip transaction timer</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The amount of time, in milliseconds that the BluStar 8000i allows the callserver (registrar/proxy) to respond to SIP messages that it sends. If the BluStar 8000i does not receive a response in the amount of time designated for this parameter, the BluStar 8000i assumes the message has timed out.
Format	Integer
Default Value	4000
Range	4000 to 64000
Example	sip transaction timer: 6000

Directory Settings

Parameter – <i>directory 1</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	<p>The name of the global directory list that you can download from the configuration server.</p> <p>Notes: You can use this parameter in three ways:</p> <ul style="list-style-type: none"> • To download no directory • To download a directory from the original configuration server • To download a directory from another specified server <p>To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example:</p> <p>directory 1: ftp://10.30.102.158/path/global.csv</p> <p>where “path” is the directory and “global.csv” is the filename. If you do not specify a filename, the download fails.</p> <p>See examples for each below.</p>
Format	Alphanumeric characters
Default Value	NA
Range	NA
Example	<p>The following example downloads no directory:</p> <p>directory 1:</p> <p>The following example downloads a company global directory from the original configuration server:</p> <p>directory 1: global.csv</p> <p>The following example downloads a company global directory file from the specified server in the “path” directory:</p> <p>directory 1: ftp://10.30.102.158/path/global.csv</p>

Parameter – <i>directory 2</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	<p>The name of a user directory list that you can download from the configuration server.</p> <p>You can use this parameter in three ways:</p> <ul style="list-style-type: none"> • To download no directory • To download a directory from the original configuration server • To download a directory from another specified server <p>To download a specific file, the string value MUST HAVE A FILENAME at the end of the string. For example:</p> <p>directory 1: ftp://10.30.102.158/path/user.csv</p> <p>where “path” is the directory and “user.csv” is the filename. If you do not specify a filename, the download fails.</p> <p>See examples for each below.</p>
Format	Alphanumeric characters
Default Value	NA
Range	NA
Example	<p>The following example downloads no directory:</p> <p>directory 2:</p> <p>The following example downloads a company directory from the original configuration server:</p> <p>directory 2: joe.csv</p> <p>The following example downloads a company directory file from the specified server in the “path” directory:</p> <p>directory 2: ftp://10.30.102.158/path/joe.csv</p>

Parameter – <i>contact dynamic search threshold</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	This parameter indicates the threshold value where the contact search is no longer dynamic. If the LDAP or Exchange directory holds more records than the configured value, the user must press the search button in order to trigger the search within the contacts.
Format	Integer
Default Value	5000
Range	0-1000000
Example	contact dynamic search threshold: 10000

Call History Settings

Parameter – <i>callers list disabled</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables call history. If this parameter is set to '0', the history screen can be accessed by all users. If this parameter is set to '1', the BluStar 8000i does not save any caller information to the call history.
Format	Boolean
Default Value	0 (false)
Range	0-1 0 (false) 1 (true)
Example	callers list disabled: 1

Missed Calls Indicator Settings

Parameter – <i>missed calls indicator disabled</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables the missed calls indicator. If the "missed calls indicator disabled" parameter is set to 0, the indicator increments as unanswered calls come into the BluStar 8000i. If the "missed calls indicator disabled" parameter is set to 1, the indicator is disabled and will NOT increment as unanswered calls come into the BluStar 8000i.
Format	Boolean
Default Value	0 (false)
Range	0-1 0 (false) 1 (true)
Example	missed calls indicator disabled: 1

Basic LDAP Settings

Parameter – <i>ldap name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the name of the LDAP directory. It is the label that will be displayed in the directory screen to identify the content, usually the company name or "corporate".
Format	String
Default Value	NA
Range	NA
Example	ldap name: acme

Parameter – <i>ldap server</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP server hostname or IP address. This parameter handles multiple values, in the format “username:password@ldapserver:port”, where: <ul style="list-style-type: none"> • user name for authentication (optional, if not provided anonymous connection will be used) • password for authentication (optional) • ldapserver is the IP address or name of the LDAP server (mandatory) • port is the LDAP interface port (optional, default is 389)
Format	String (hostname or IP address)
Default Value	NA
Range	NA
Example	ldap server: ldap.company.com (no authentication and using default port 389) ldap server: user:password@ldap.company.com:3268 (authentication and using port 3268)

Parameter – <i>ldap base dn</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP server base DN. It is the description of the top level of the directory tree. Usually if a company domain is “company.com”, the base DN (distinguished name) must be entered under the form “dc=company, dc=com”.
Format	String
Default Value	NA
Range	NA
Example	ldap base dn: dc=acme, dc=com (for acme.com)

Parameter – <i>enable user defined ldap</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	This administrator parameter allows (or disallows) the user to edit his LDAP directory configuration overriding the configuration coming from the configuration server.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	enable user defined ldap: 1

Advanced LDAP Settings

Parameter – <i>ldap name title attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP name title (e.g. Mr.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap name title attribute list: title, gender

Parameter – <i>ldap first name attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP first name (e.g. John) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap first name attribute list: fname, uname

Parameter – <i>ldap last name attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP last name (e.g. Doe) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap last name attribute list: name, lname

Parameter – <i>ldap middle name attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP middle name (e.g. Allen) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap middle name attribute list: mname, initial

Parameter – <i>ldap name suffix attribute</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP name suffix (e.g. Ph.D) for the attribute list. If this parameter contains more than one value, only the first matching value will be picked in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap name suffix attribute: suffix

Parameter – <i>ldap company attribute list</i>	Configuration Files – astra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP company name (e.g. Aastra) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap company attribute list: organization, bname

Parameter – <i>ldap job title attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP job title (e.g. Vice President) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap job title attribute list: jtitle, title

Parameter – <i>ldap business street attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business street (e.g. Snow Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business street attribute list: waddress, baddress

Parameter – <i>ldap business city attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business city (e.g. Concord) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business city attribute list: wcity, bcity

Parameter – <i>ldap business state attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business state (e.g. Ontario) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business state attribute list: wstate, bstate

Parameter – <i>ldap business postal code attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business postal code (e.g. L4K 4N9) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business postal code attribute list: bcode, wcode

Parameter – <i>ldap business country attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business country (e.g. Canada) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business country attribute list: bcountry, wcountry

Parameter – <i>ldap home street attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP home street (e.g. Internet Blvd.) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap home street attribute list: hstreet, pstreet

Parameter – <i>ldap home city attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP home city (e.g. Frisco) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap home city attribute list: hcity, pcity

Parameter – <i>ldap home state attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP home state (e.g. Texas) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap home state attribute list: hstate, pstate

Parameter – <i>ldap home postal code attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP home postal code (e.g. 75034) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap home postal code attribute list: hcode, pcode

Parameter – <i>ldap home country attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP home country (e.g. U.S.A) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap home country attribute list: hcountry, pcountry

Parameter – <i>ldap business phone 1 attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business phone 1 (e.g. 1-905-760-4200) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business phone 1 attribute list: wphone1, bphone1

Parameter – <i>ldap business phone 2 attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business phone 2 (e.g. 1-905-760-4201) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business phone 2 attribute list: wphone2, bphone2

Parameter – <i>ldap home phone 1 attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP home phone 1 (e.g. 1-416-468-3266) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap home phone 1 attribute list: hphone1, pphone1

Parameter – <i>ldap home phone 2 attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP home phone 2 (e.g. 1-416-468-3267) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap home phone 2 attribute list: hphone2, pphone2

Parameter – <i>ldap mobile phone attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP mobile phone (e.g. 1-416-468-3268) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap mobile phone attribute list: cell, mobile

Parameter – <i>ldap other phone attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP other phone (e.g. 1-416-468-3269) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap other phone attribute list: otherphone, mphone

Parameter – <i>ldap business fax attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP business fax (e.g. 1-905-760-4233) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap business fax attribute list: fax, bfax

Parameter – <i>ldap email 1 attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP email 1 (e.g. john.doe@aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap email 1 attribute list: email1, mail1

Parameter – <i>ldap email 2 attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP email 2 (e.g. john.d@aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap email 2 attribute list: email2, mail2

Parameter – <i>ldap email 3 attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP email 3 (e.g. j.doe@aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap email 3 attribute list: email3, mail3

Parameter – <i>ldap web address attribute list</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the LDAP web address (e.g. www.aastra.com) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
Format	String, list of attribute names separated by a comma.
Default Value	NA
Range	NA
Example	ldap web address attribute list: web, url

Parameter – <i>ldap cn attribute</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used when both the first and last name of a record are empty
Format	String
Default Value	NA
Range	NA
Example	ldap cn attribute: display

Parameter – <i>ldap dn attribute</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used to perform the search request for the detailed view of an LDAP contact.
Format	String
Default Value	NA
Range	NA
Example	ldap dn attribute: customDN

Parameter – <i>ldap dn query mode</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies which method to use when an individual record is looked up. If configured as “filter”, the BluStar 8000i performs a DN search using the root base DN with the filter “(dn=XXXX)”. If configured as “base”, the BluStar 8000i performs a DN search using the searched DN as a base with a filter defined in the parameter “ldap dn base query filter” and a scope defined in the parameter “ldap dn base query scope”. Note: This parameter is ignored if the LDAP directory is a Microsoft Active Directory.
Format	String list filter/base
Default Value	filter
Range	filter/base
Example	ldap dn query mode: base

Parameter – <i>ldap dn base query filter</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Filter used when an individual record is looked up if the parameter “ldap dn query mode” is set to “base”. Note: This parameter is ignored if the LDAP directory is a Microsoft Active Directory.
Format	String
Default Value	(objectClass=*)
Range	NA
Example	ldap dn base query filter: (objectClass=*)

Parameter – <i>ldap dn base query scope</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Scope used when an individual record is looked up if the parameter “ldap dn query mode” is set to “base”. A “base” search is performed only on the base DN, a “onelevel” search is performed on the base DN and the first sublevel, and a “subtree” search is performed on the whole tree under the base DN. Note: This parameter is ignored if the LDAP directory is a Microsoft Active Directory.
Format	String list base/onelevel/subtree
Default Value	subtree
Range	base/onelevel/subtree
Example	ldap dn base query scope: onellevel

Parameter – <i>ldap search filter</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used to set search filters. This parameter format must follow RFC 4515, for example (sn=%). This parameter must include a '%' character at the place where it will be replaced by a*, b*, etc...
Format	String
Default Value	NA
Range	NA
Example	ldap search filter: (&(sn=*)(number=*))

Parameter – <i>ldap search scope</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used to set the search scope. A "base" search is performed only on the baseDN, a "onelevel" search is performed on the baseDN and the first sub-level, and a "subtree" search is performed on the whole tree under the base DN.
Format	String list base/onelevel/subtree
Default Value	NA
Range	base/onelevel/subtree
Example	ldap search scope: onellevel

Parameter – <i>ldap search timeout</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used to set the request timeout for LDAP requests.
Format	Integer, seconds
Default Value	NA
Range	1 to 120
Example	ldap search timeout: 30

Parameter – <i>ldap network timeout</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used to set the network timeout for LDAP requests.
Format	Integer, seconds
Default Value	NA
Range	1 to 120
Example	ldap network timeout: 50

Parameter – <i>ldap initial download delay</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Used to set the LDAP initial download delay. Setting a value of 0 does not introduce any delay and the initial download is performed synchronously during the login process. With all other values, the download is performed asynchronously, delayed by the value amount (in seconds) after the login process.
Format	Integer, seconds
Default Value	NA
Range	0 to 120
Example	ldap initial download delay: 60

Microsoft Exchange Contact Settings

Parameter – <i>enable user defined exchange contacts</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether to enable or disable a user's ability to edit his or her Microsoft Exchange contacts configuration.
Format	Boolean
Default Value	0 (disabled)
Range	0 -1 0 (disabled) 1 (enabled)
Example	enable user defined exchange contacts: 1

Parameter – <i>exchange contacts enabled</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies whether a user's Microsoft Exchange contacts should be synced with the terminal's address book. When enabled, the user will not be able to access the personal contacts that have been set up by the administrator.
Format	Boolean
Default Value	0 (disabled)
Range	0 -1 0 (disabled) 1 (enabled)
Example	exchange contacts enabled: 1

Parameter – <i>exchange email</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the user's Microsoft Exchange email address.
Format	String
Default Value	NA
Range	NA
Example	exchange email: john.doe@acme.com

Parameter – <i>exchange server ip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the user's Microsoft Exchange server IP address or Fully Qualified Domain Name (FQDN).
Format	IP address or FQDN
Default Value	0.0.0.0
Range	NA
Example	exchange server ip: mail.acme.com

Parameter – <i>exchange user domain</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the user's Microsoft Exchange domain name.
Format	String
Default Value	NA
Range	NA
Example	exchange user domain: acme

Parameter – <i>exchange contact folder name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the optional custom folder that will be used to store the user's Microsoft Exchange contacts.
Format	String
Default Value	NA
Range	NA
Example	exchange contact folder name: Exchange

Parameter – <i>exchange use login credentials</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies whether the user's BluStar 8000i user name and password is the same the user's Microsoft Exchange user name and password (enabled) or if login credentials should be manually input (disabled).
Format	Boolean
Default Value	0 (disabled)
Range	0 -1 0 (disabled) 1 (enabled)
Example	exchange use login credentials: 1

Parameter – <i>exchange username</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the user's Microsoft Exchange user name. This parameter is only used if the parameter " exchange use login credentials " is set to disabled.
Format	String
Default Value	NA
Range	NA
Example	exchange username: jdoe

Parameter – <i>exchange password</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	<p>Specifies the user's Microsoft Exchange password. This parameter is only used if the parameter "exchange use login credentials" is set to disabled.</p> <p>Note: The "exchange password" parameter is available in the user.cfg file, but the password string will be encrypted. The password can only be input by the user through the contacts menu on the user's respective BluStar 8000i terminal.</p>
Format	NA
Default Value	NA
Range	NA
Example	NA

Parameter – <i>exchange ssl enabled</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies whether SSL (Secure Sockets Layer) should be enabled or disabled.
Format	Boolean
Default Value	0 (disabled)
Range	0 -1 0 (disabled) 1 (enabled)
Example	exchange ssl enabled: 1

LDAP Directory/Exchange Contacts Update Interval

Parameter – <i>ldap resync time</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Sets the time of day in a 24-hour period for the BluStar 8000i terminal to automatically update the LDAP directory. Notes: <ul style="list-style-type: none"> • The resync time is based on the local time of the terminal. • LDAP directory resync will occur any time between the values set for the "ldap resync time" and "ldap resync max delay" parameters. For example, if the "ldap resync time" parameter is set to 02:00 and the "ldap resync max delay" is set to 30, the update will take place any time between 02:00 and 02:30 • The value of 00:00 is 12:00 A.M.
Format	HH:MM (24 hours)
Default Value	02:00
Range	HH=00 to 23, MM=0 to 59
Examples	ldap resync time: 03:15

Parameter – <i>ldap resync days</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the amount of days that the terminal waits between resync operations for the LDAP directory. Note: A value of 0 causes the terminal to resync every time the clock reads the proper time, a value of 1 forces the terminal to wait 24 hours prior to doing the first resync.
Format	Integer
Default Value	0
Range	0 to 364
Examples	ldap resync days: 1

Parameter – <i>ldap resync max delay</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum time, in minutes, the terminal waits past the scheduled time before starting a resync for the LDAP directory.
Format	Integer
Default Value	30
Range	0 to 1439
Examples	ldap resync max delay: 60

Parameter – <i>exchange contacts resync time</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Sets the time of day in a 24-hour period for the BluStar 8000i terminal to automatically update the Exchange contacts.</p> <p>Notes:</p> <ul style="list-style-type: none"> • The resync time is based on the local time of the terminal. • Exchange contacts resync will occur any time between the values set for the "exchange contacts resync time" and "exchange contacts resync max delay" parameters. For example, if the "exchange contacts resync time" parameter is set to 02:00 and the "exchange contacts resync max delay" is set to 30, the update will take place any time between 02:00 and 02:30. The value of 00:00 is 12:00 A.M.
Format	HH:MM (24 hours)
Default Value	02:00
Range	HH=00 to 23, MM=0 to 59
Examples	exchange contacts resync time: 03:15

Parameter – <i>exchange contacts resync days</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Specifies the amount of days that the terminal waits between resync operations for the Exchange contacts.</p> <p>Note: A value of 0 causes the terminal to resync every time the clock reads the proper time, a value of 1 forces the terminal to wait 24 hours prior to doing the first resync.</p>
Format	Integer
Default Value	0
Range	0 to 364
Examples	exchange contacts resync days: 1

Parameter – <i>exchange contacts resync max delay</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum time, in minutes, the terminal waits past the scheduled time before starting a resync for the Exchange contacts.
Format	Integer
Default Value	30
Range	0 to 1439
Examples	exchange contacts resync max delay: 60

User Settings

Parameter – <i>user config upload</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Number of seconds until settings or contacts will be re-uploaded to the server IF there has been a change.
Format	Integer
Default Value	3600
Range	0 -16400
Example	user config upload: 4800

Power Saving Schedule Settings

Use the following parameters to configure the power saving schedule:

Parameter – <i>user defined power savings schedule</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not users are allowed to configure the power saving schedule on their BluStar 8000i. If enabled, users will be allowed to configure their own power saving schedule.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	user defined power savings schedule: 0

Parameter – <i>working monday</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not Mondays are part of the BluStar 8000i user's normal work week.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working monday: 1

Parameter – <i>working tuesday</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not Tuesdays are part of the BluStar 8000i user's normal work week.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working tuesday: 1

Parameter – <i>working wednesday</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not Wednesdays are part of the BluStar 8000i user's normal work week.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working wednesday: 1

Parameter – <i>working thursday</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not Thursdays are part of the BluStar 8000i user's normal work week.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working thursday: 1

Parameter – <i>working friday</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not Fridays are part of the BluStar 8000i user's normal work week.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working friday: 1

Parameter – <i>working saturday</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not Saturdays are part of the BluStar 8000i user's normal work week.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working saturday: 0

Parameter – <i>working sunday</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not Sundays are part of the BluStar 8000i user's normal work week.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working sunday: 0

Parameter – <i>working all days</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not the BluStar 8000i user's normal work week consists of all the days of the week.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	working all days: 0

Parameter – <i>working hour weekday start</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the starting hour of the BluStar 8000i user's weekday work schedule. Note: The term "weekday" refers to the days from Monday to Friday.
Format	Text
Default Value	6
Range	Dependent on the time format of the respective BluStar 8000i. 1-12 (if time format is 12 hour) 0-23 (if time format is 24 hour)
Example	working hour weekday start: 9

Parameter – <i>working minute weekday start</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the starting minute of the BluStar 8000i user's weekday work schedule. Note: The term "weekday" refers to the days from Monday to Friday.
Format	Text
Default Value	0
Range	0-59
Example	working minute weekday start: 15

Parameter – <i>working pm weekday start</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether the BluStar 8000i user's weekday work schedule start time defined in the "working hour weekday start" and "working minute weekday start" parameters is AM or PM. Notes: <ul style="list-style-type: none"> • This parameter should only be used if the BluStar 8000i is using the 12-hour time format. • The term "weekday" refers to the days from Monday to Friday.
Format	Boolean
Default Value	0 (AM)
Range	0-1 0 (AM) 1 (PM)
Example	working pm weekday start: 0

Parameter – <i>working hour weekday end</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the ending hour of the BluStar 8000i user's weekday work schedule. Note: The term "weekday" refers to the days from Monday to Friday.
Format	Text
Default Value	10
Range	Dependent on the time format of the respective BluStar 8000i. 1-12 (if time format is 12 hour) 0-23 (if time format is 24 hour)
Example	working hour weekday end: 5

Parameter – <i>working minute weekday end</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the ending minute of the BluStar 8000i user's weekday work schedule. Note: The term "weekday" refers to the days from Monday to Friday.
Format	Text
Default Value	0
Range	0-59
Example	working minute weekday end: 30

Parameter – <i>working pm weekday end</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether the BluStar 8000i user's weekday work schedule end time defined in the "working hour weekday end" and "working minute weekday end" parameters is AM or PM. Notes: <ul style="list-style-type: none"> • This parameter should only be used if the BluStar 8000i is using the 12-hour time format. • The term "weekday" refers to the days from Monday to Friday.
Format	Boolean
Default Value	1 (PM)
Range	0-1 0 (AM) 1 (PM)
Example	working pm weekday end: 1

Parameter – <i>working hour weekend start</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the starting hour of the BluStar 8000i user's weekend work schedule. Note: The term "weekend" refers to Saturday and Sunday.
Format	Text
Default Value	0
Range	Dependent on the time format of the respective BluStar 8000i. 1-12 (if time format is 12 hour) 0-23 (if time format is 24 hour)
Example	working hour weekend start: 11

Parameter – <i>working minute weekend start</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the starting minute of the BluStar 8000i user's weekend work schedule. Note: The term "weekend" refers to Saturday and Sunday.
Format	Text
Default Value	0
Range	0-59
Example	working minute weekend start: 30

Parameter – <i>working pm weekend start</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether the BluStar 8000i user's weekend work schedule start time defined in the "working hour weekend start" and "working minute weekend start" parameters is AM or PM. Note: <ul style="list-style-type: none"> This parameter should only be used if the BluStar 8000i is using the 12-hour time format. The term "weekend" refers to Saturday and Sunday.
Format	Boolean
Default Value	0 (AM)
Range	0-1 0 (AM) 1 (PM)
Example	working pm weekend start: 0

Parameter – <i>working hour weekend end</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the ending hour of the BluStar 8000i user's weekend work schedule. Note: The term "weekend" refers to Saturday and Sunday.
Format	Text
Default Value	0
Range	Dependent on the time format of the respective BluStar 8000i. 1-12 (if time format is 12 hour) 0-23 (if time format is 24 hour)
Example	working hour weekend end: 3

Parameter – <i>working minute weekend end</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the ending minute of the BluStar 8000i user's weekend work schedule. Note: The term "weekend" refers to Saturday and Sunday.
Format	Text
Default Value	0
Range	0-59
Example	working minute weekend end: 30

Parameter – <i>working pm weekend end</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether the BluStar 8000i user's weekend work schedule end time defined in the "working hour weekend end" and "working minute weekend end" parameters is AM or PM. Note: <ul style="list-style-type: none"> This parameter should only be used if the BluStar 8000i is using the 12-hour time format. The term "weekend" refers to Saturday and Sunday.
Format	Boolean
Default Value	1 (PM)
Range	0-1 0 (AM) 1 (PM)
Example	working pm weekend end: 1

Parameter – <i>weekend working same as week-days</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies whether or not the BluStar 8000i user's weekend work schedule is the same as his/her weekday work schedule. Note: The term "weekday" for the Power Saving Schedule feature on the BluStar 8000i refers to the days from Monday to Friday. The term "weekend" refers to Saturday and Sunday.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	weekend working same as weekdays: 0

Terminal Security Settings

Parameter – <i>require settings password</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies if a password should be required to edit the BluStar 8000i terminal identity.
Format	Boolean
Default Value	0 (disabled)
Range	0 -1 0 (disabled) 1 (enabled)
Example	require settings password: 1

Parameter – <i>settings password</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the password required to edit the BluStar 8000i terminal identity if the “require settings password” parameter is enabled.
Format	String
Default Value	aastra
Range	Up to 30 alpha-numeric characters.
Example	settings password: blustar123

Parameter – <i>logoff disable dial</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Allows administrators to disable dialing when logged off.
Format	Integer
Default Value	0
Range	0-1 0 (no) 1 (yes)
Example	logoff disable dial: 1

Parameter – <i>auto answer</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Allows administrators to change the automatic answer settings. Note: This parameter affects all auto-answer features including auto-answer of incoming intercom calls.
Format	Integer
Default Value	0
Range	0-1 0 (no) 1 (yes)
Example	auto answer: 1

Parameter – <i>auto reboot</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	The time at which the devices reboot. To auto reboot ASAP, use current date and time.
Format	yyyy-mm-dd hh:mm:ss
Default Value	NA
Range	NA
Example	auto reboot: 2011-12-13 12:34:56

Parameter – <i>screen lock time</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Can be set to 0 and the unit of time (e.g. “0 seconds”) to disable or to a specified number of seconds, minutes, hours, or days. The screen locks after the set value. Note: When setting the value for this parameter, the unit of time must be specified and can be in singular or plural form.
Format	String
Default Value	0 second(s)/minute(s)/hour(s)/day(s) (disabled)
Range	0 second(s)/minute(s)/hour(s)/day(s) (disabled) 1-10000 second(s)/minute(s)/hour(s)/day(s)
Example	screen lock time: 30 seconds

Screen Settings

Screen Dimming Settings

Parameter – <i>screen 1st dim time</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Can be set to 0 and the unit of time (e.g. “0 seconds”) to disable or to a specified number of seconds, minutes, hours, or days. The screen <i>partially</i> dims after the set value. Note: When setting the value for this parameter, the unit of time must be specified and can be in singular or plural form.
Format	String
Default Value	300 seconds
Range	0 second(s)/minute(s)/hour(s)/day(s) (disabled) 1-10000 second(s)/minute(s)/hour(s)/day(s)
Example	screen 1st dim time: 60 seconds

Parameter – <i>screen 2nd dim time</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Can be set to 0 and the unit of time (e.g. “0 seconds”) to disable or to a specified number of seconds, minutes, hours, or days. The screen <i>further</i> dims after the set value. Note: When setting the value for this parameter, the unit of time must be specified and can be in singular or plural form.
Format	String
Default Value	0 second(s)/minute(s)/hour(s)/day(s) (disabled)
Range	0 second(s)/minute(s)/hour(s)/day(s) (disabled) 1-10000 second(s)/minute(s)/hour(s)/day(s)
Example	screen 2nd dim time: 5 minutes

Screen Saver Settings

Parameter – <i>screen save time</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Can be set to 0 and the unit of time (e.g. “0 seconds”) to disable or to a specified number of seconds, minutes, hours, or days. The screen saver enables after the set value. Note: When setting the value for this parameter, the unit of time must be specified and can be in singular or plural form.
Format	String
Default Value	0 second(s)/minute(s)/hour(s)/day(s) (disabled)
Range	0 second(s)/minute(s)/hour(s)/day(s) (disabled) 1-10000 second(s)/minute(s)/hour(s)/day(s)
Example	screen save time: 2 hours

Show Cursor Settings

Parameter – <i>show cursor</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Displays the mouse cursor.
Format	Integer
Default Value	0
Range	0-1 0 (no) 1 (yes)
Example	show cursor: 1

Locale Settings

Parameter – <i>language name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the language you want to display on the BluStar 8000i.
Format	String
Default Value	English
Range	English French German Italian Japanese Simplified Chinese Spanish Note: Language values are case sensitive and are entered in English only.
Example	language name: French

Parameter – <i>time zone name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the time zone on the BluStar 8000i.
Format	String
Default Value	us-eastern
Range	See Time Zone Name Table below for specific time zone names.
Example	time zone name: us-eastern

Time Zone Name Table

Time Zone Names			
AD-Andorra	BA-Sarajevo	CA-Newfoundland	DE-Berlin
AE-Dubai	BB-Barbados	CA-Atlantic	DK-Copenhagen
AG-Antigua	BE-Brussels	CA-Eastern	DM-Dominica
AI-Anguilla	BG-Sofia	CA-Saskatchewan	DO-Santo Domingo
AL-Tirane	BM-Bermuda	CA-Central	Dhcp
AN-Curacao	BO-La Paz	CA-Mountain	
AR-Buenos Aires	BR-Noronha	CA-Pacific	
AR-San Luis	BR-Belem	CA-Yukon	
AS-Pago Pago	BR-Fortaleza	CH-Zurich	
AT-Vienna	BR-Recife	CK-Rarotonga	
AU-Lord Howe	BR-Araguaina	CL-Santiago	
AU-Tasmania	BR-Maceio	CL-Easter	
AU-Melbourne	BR-Sao Paulo	CN-China	
AU-Sydney	BR-Cuiaba	CO-Bogota	
AU-Broken Hill	BR-Porto Velho	CR-Costa Rica	
AU-Brisbane	BR-Boa Vista	CU-Havana	
AU-Lindeman	BR-Manaus	CY-Nicosia	
AU-Adelaide	BR-Eirunepe	CZ-Prague	
AU-Darwin	BR-Rio Branco		
AU-Perth	BS-Nassau		
AW-Aruba	BY-Minsk		
AZ-Baku	BZ-Belize		
EE-Tallinn	FI-Helsinki	GB-London	HK-Hong Kong
ES-Madrid	FJ-Fiji	GB-Belfast	HN-Tegucigalpa
ES-Canary	FK-Stanley	GD-Grenada	HR-Zagreb
	FO-Faeroe	GE-Tbilisi	HT-Port-au-Prince
	FR-Paris	GF-Cayenne	HU-Budapest
		GI-Gibraltar	
		GP-Guadeloupe	
		GR-Athens	
		GS-South Georgia	
		GT-Guatemala	
		GU-Guam	
		GY-Guyana	
IE-Dublin	JM-Jamaica	KY-Cayman	LC-St Lucia
IS-Reykjavik	JP-Tokyo		LI-Vaduz
IT-Rome			LT-Vilnius
			LU-Luxembourg
			LV-Riga

Time Zone Names			
MC-Monaco	NI-Managua	OM-Muscat	PA-Panama
MD-Chisinau	NL-Amsterdam		PE-Lima
MK-Skopje	NO-Oslo		PL-Warsaw
MQ-Martinique	NR-Nauru		PR-Puerto Rico
MS-Montserrat	NU-Niue		PT-Lisbon
MT-Malta	NZ-Auckland		PT-Madeira
MU-Mauritius	NZ-Chatham		PT-Azores
MX-Mexico City			PY-Asuncion
MX-Cancun			
MX-Merida			
MX-Monterrey			
MX-Mazatlan			
MX-Chihuahua			
MX-Hermosillo			
MX-Tijuana			
RO-Bucharest	SA-Saudi Arabia	TR-Istanbul	UA-Kiev
RU-Kaliningrad	SE-Stockholm	TT-Port of Spain	US-Eastern
RU-Moscow	SG-Singapore	TW-Taipei	US-Central
RU-Samara	SI-Ljubljana		US-Mountain
RU-Yekaterinburg	SK-Bratislava		US-Pacific
RU-Omsk	SM-San Marino		US-Alaska
RU-Novosibirsk	SR-Paramaribo		US-Aleutian
RU-Krasnoyarsk	SV-El Salvador		US-Hawaii
RU-Irkutsk			UY-Montevideo
RU-Yakutsk			
RU-Vladivostok			
RU-Sakhalin			
RU-Magadan			
RU-Kamchatka			
RU-Anadyr			
VA-Vatican	YU-Belgrade		
VE-Caracas			

Parameter – <i>date format</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	This parameter allows the user to change the date displayed on the home screen, in all applications, and in the call logs to various formats. Note: If a date format is selected that contains the year, the home screen will not display the year due to space limitations.
Format	Integer
Default Value	0
Range	0 (WWW MMM DD) (default) 1 (DD-MMM-YY) 2 (YYYY-MM-DD) 3 (DD/MM/YYYY) 4 (DD/MM/YY) 5 (DD-MM-YY) 6 (MM/DD/YY) 7 (MMM DD) 8 (DD MMM YYYY) 9 (WWW DD MMM) 10 (DD MMM) 11 (DD.MM.YYYY)
Example	date format: 7

Parameter – <i>time format</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	This parameter changes the time displayed on the home screen, in all applications, and in the call logs to a 12 hour or 24 hour format. Use "0" for a 12 hour format and "1" for a 24 hour format.
Format	Integer
Default Value	0
Range	0 (12 hr format) 1 (24 hr format)
Example	time format: 1

Audio/Video Settings

Parameter – <i>video max kbitrate</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum video bandwidth limit.
Format	Integer
Default Value	Dynamic
Range	5000, 3000, 2500, 1500, 768, 384, 128
Example	video max kbitrate: 3000

Parameter – <i>audio max kbitrate</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum audio bandwidth limit.
Format	Integer
Default Value	Dynamic
Range	64, 32, 24, 16
Example	audio max kbitrate: 24

Parameter – <i>user defined video rate</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	This administrator parameter allows (or disallows) users the ability to change their maximum video data transmit and receive rates allowed for calls with BluStar 8000i or non-BluStar 8000i devices.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	user defined video rate: 0

Parameter – <i>max 8000i h.264 tx rate</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum video data transmit rate allowed when in a call with BluStar 8000i devices.
Format	Integer
Default Value	6000
Range	5000, 2500, 1500, 768, 512, 384, 128
Example	max 8000i h.264 tx rate: 2500

Parameter – <i>max 8000i h.264 rx rate</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum video data receive rate allowed when in a call with BluStar 8000i devices.
Format	Integer
Default Value	6000
Range	5000, 2500, 1500, 768, 512, 384, 128
Example	max 8000i h. 264 rx rate: 2500

Parameter – <i>max h.264 tx rate</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum video data transmit rate allowed when in a call with non-BluStar 8000i devices.
Format	Integer
Default Value	768
Range	3000, 1920, 1536, 1024, 768, 512, 384, 128
Example	max h.264 tx rate: 512

Parameter – <i>max h.264 rx rate</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the maximum video data receive rate allowed when in a call with non-BluStar 8000i devices.
Format	Integer
Default Value	768
Range	3000, 1920, 1536, 1024, 768, 512, 384, 128
Example	max h.264 rx rate: 512

Call Forward Settings

Parameter – <i>call forward disabled</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Enables or disables the ability to configure Call Forwarding. If this parameter is set to '0', a user and administrator can configure Call Forwarding via the BluStar 8000i UI from the "Call Handling" screen in the Tools menu. If this parameter is set to '1', all "Call Forward" options are removed from the BluStar 8000i UI, preventing the ability to configure Call Forwarding.
Format	Boolean
Default Value	0 (false)
Range	0 - 1 0 (false) 1 (true)
Example	call forward disabled: 1

Parameter – <i>sip forward all state</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	If call forward all state is ON, then the Call Forward All settings will be used in normal scenarios. Note: The “sip forward all number” parameter must be set.
Format	Boolean
Default Value	0
Range	0-1 0 (off) 1 (on)
Example	sip forward all state: 1

Parameter – <i>sip forward all number</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the Call Forward All number. Note: The “sip forward all state” parameter must be set.
Format	String (number or URL)
Default Value	NA
Range	NA
Example	sip forward all number: 2134

Parameter – <i>sip forward busy state</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	If call forward busy state is ON, then the Call Forward Busy settings will be used in normal scenarios. Note: The “sip forward busy number” parameter must be set.
Format	Boolean
Default Value	0
Range	0-1 0 (off) 1 (on)
Example	sip forward busy state: 1

Parameter – <i>sip forward busy number</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the Call Forward Busy number. Note: The “sip forward busy state” parameter must be set.
Format	String (number or URL)
Default Value	NA
Range	NA
Example	sip forward busy number: 4123

Parameter – <i>sip forward no answer state</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	If call forward no answer state is ON, then the Call Forward No Answer settings will be used in normal scenarios. Note: The “sip forward no answer number” and “sip ring number” parameters must also be set.
Format	Boolean
Default Value	0
Range	0-1 0 (off) 1 (on)
Example	sip forward no answer state: 1

Parameter – <i>sip forward no answer number</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the Call Forward No Answer number. Note: The “sip forward no answer state” parameter must be ON and the “sip ring number” parameter must be set.
Format	String (number or URL)
Default Value	NA
Range	NA
Example	sip forward no answer number: 3523

Parameter – <i>sip ring number</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the number of rings until the call will be forwarded if there is no answer. Note: The “sip forward no answer state” parameter must be ON and the “sip forward no answer number” parameter must be set.
Format	Integer
Default Value	3
Range	1-10
Example	sip ring number: 5

Incoming Intercom Call Auto-Answer Settings

Parameter – <i>sip allow auto answer</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables/disables the auto-answer feature for incoming intercom calls. If enabled, the BluStar 8000i terminal will recognize an incoming intercom call by the information relayed in the “Call-Info” header of the SIP INVITE and automatically answer the call. If disabled, the phone will treat the intercom call as if it is a normal incoming call. Note: The parameter “auto answer” must be enabled for this parameter to take effect.
Format	Boolean
Default Value	1
Range	0-1 0 (no) 1 (yes)
Example	sip allow auto answer: 0

Voicemail Settings

Parameter – <i>sip vmail</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies the phone number of the voicemail system connected to the SIP account. This parameter specifies the phone number you dial from your BluStar 8000i to retrieve your voicemail.
Format	Integer
Default Value	NA
Range	NA
Example	sip vmail: 5000

Video Voicemail Client Integration Settings

Parameter – <i>voicemail integration url</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The url (http or https) the BluStar 8000i calls to perform voicemail integration. Note: The parameter “sip xml notify event” must be enabled to ensure full functionality of the video voicemail client.
Format	String
Default Value	N/A
Range	N/A
Example	voicemail integration url: http://myserver.com/integration.php

Parameter – <i>voicemail integration use login credentials</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	By default the BluStar 8000i uses SIP credentials to authenticate (digest method) to the voicemail integration server. Enabling this configuration parameter makes the BluStar 8000i use the user login/password instead.
Format	Boolean
Default Value	0
Range	0-1 0 (disabled) 1 (enabled)
Example	voicemail integration use login credentials: 1

Parameter – <i>voicemail integration needs sip registration</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used by the voicemail integration API to indicate to the software if SIP registration is needed before sending a user command via the API. When enabled, the BluStar 8000i checks the extension registration status before sending an API command. If the extension is not registered, an error message is displayed.
Format	Boolean
Default Value	0
Range	0-1 0 (disabled) 1 (enabled)
Example	voicemail integration needs sip registration: 1

Emergency Dial Plan Settings

Parameter – <i>emergency dial plan</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg												
Description	<p>Allows you to specify an emergency number to use on your BluStar 8000i so a caller can contact emergency services in the local area even when the terminal is locked.</p> <p>The default emergency numbers on the BluStar 8000i are 911, 999, 112, and 110.</p> <p>911 - A United States emergency number. 999 - A United Kingdom emergency number. 112 - An international emergency telephone number for GSM mobile phone networks. In all European Union countries it is also the emergency telephone number for both mobile and fixed-line telephones. 110 - A police and/or fire emergency number in Asia, Europe, Middle East, and South America.</p> <table> <thead> <tr> <th>Dial plan (characters)</th><th>Length (bytes)</th></tr> </thead> <tbody> <tr> <td>911</td><td>14</td></tr> <tr> <td>4xx</td><td>18</td></tr> <tr> <td>x+## xx+*</td><td>35</td></tr> <tr> <td>911 999 112 110 450</td><td>54</td></tr> <tr> <td>911 112 011XX+## 101XX+## 1[2-3]XXXXXXXXXX [4-5]XXXXXXXXXX [6-7]XXXXXXXXXX,3 [8-9]XXXXXXXXXX,2 XX+* XX+## *XXX+## ##XX+## 4xx,2</td><td>325</td></tr> </tbody> </table> <p>Note: Contact your local phone service provider for available emergency numbers in your area.</p>	Dial plan (characters)	Length (bytes)	911	14	4xx	18	x+## xx+*	35	911 999 112 110 450	54	911 112 011XX+## 101XX+## 1[2-3]XXXXXXXXXX [4-5]XXXXXXXXXX [6-7]XXXXXXXXXX,3 [8-9]XXXXXXXXXX,2 XX+* XX+## *XXX+## ##XX+## 4xx,2	325
Dial plan (characters)	Length (bytes)												
911	14												
4xx	18												
x+## xx+*	35												
911 999 112 110 450	54												
911 112 011XX+## 101XX+## 1[2-3]XXXXXXXXXX [4-5]XXXXXXXXXX [6-7]XXXXXXXXXX,3 [8-9]XXXXXXXXXX,2 XX+* XX+## *XXX+## ##XX+## 4xx,2	325												
Format	Integer												
Default Value	911 999 112 110												
Range	Up to 512 characters												
Example	emergency dial plan: 911 999												

Parameter – <i>sip emergency auth name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used in the user name field of the Authorization header field of the <i>SIP REGISTER</i> request. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip emergency auth name: 5553456

Parameter – <i>sip emergency display name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Used in the display name field of the <i>From</i> SIP header field. Some IP PBX systems use this as the caller's ID and some may overwrite this with the string that is set at the PBX system. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip emergency display name: Joe Smith

Parameter – <i>sip emergency user name</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	User name used in the name field of the <i>SIP URI</i> for the BluStar 8000i and for registering the BluStar 8000i at the registrar. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off. Note: The BluStar 8000i support user names containing dots ("").
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip emergency user name: 1010

Parameter – <i>sip emergency password</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The password that will be used to register at the registrar. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	Text
Default Value	NA
Range	Up to 20 alphanumeric characters
Example	sip emergency password: 12345

Parameter – <i>sip emergency proxy ip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The IP address of the SIP proxy server for which the BluStar 8000i uses to send all SIP requests. A SIP proxy is a server that initiates and forwards requests generated by the BluStar 8000i to the targeted user. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	IP address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	Up to 64 alphanumeric characters.
Example	sip emergency proxy ip: 192.168.0.101

Parameter – <i>sip emergency proxy port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The proxy server's port number. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	Integer
Default Value	0
Range	NA
Example	sip emergency proxy port: 5060

Parameter – <i>sip emergency outbound proxy</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	This is the address of the outbound proxy server. All SIP messages originating from the BluStar 8000i are sent to this server. For example, if you have a Session Border Controller in your network, then you would normally set its address here. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	IP Address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	NA
Example	sip emergency outbound proxy: 10.42.23.13

Parameter – <i>sip emergency outbound proxy port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The proxy port on the proxy server to which the BluStar 8000i sends all SIP messages. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	Integer
Default Value	0
Range	NA
Example	sip emergency outbound proxy port: 5060

Parameter – <i>sip emergency registrar ip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The address of the registrar for which the BluStar 8000i uses to send <i>REGISTER</i> requests. A SIP registrar is a server that maintains the location information of the BluStar 8000i. A value of 0.0.0.0 disables registration. However, the BluStar 8000i is still active and you can dial using the username@ip address of the BluStar 8000i. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	IP address or Fully Qualified Domain Name
Default Value	0.0.0.0
Range	NA
Example	sip emergency registrar ip: 192.168.0.101

Parameter – <i>sip emergency registrar port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The registrar's port number. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	Integer
Default Value	0
Range	NA
Example	sip emergency registrar port: 5060

Parameter – <i>sip emergency registration period</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The requested registration period, in seconds, from the registrar. Utilized when the emergency dial plan feature is configured and only when the terminal is logged off.
Format	Integer
Default Value	0
Range	0 - 2147483647
Example	sip emergency registration period: 3600

Picture ID Feature

Parameter – <i>image server uri</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Allows you to specify the server URI where pictures are stored for display to the BluStar 8000i during incoming and outgoing calls, and in the directory, callers list, and redial list entries. The pictures are dynamically retrieved from the centralized server for each call and then locally cached in the BluStar 8000i to reduce network traffic.</p> <p>If there is no picture on the central server for the dialed and/or caller ID number, and directory, callers list, and/or the dial list entry, the generic blue figure image is shown.</p> <p>Pictures can be in either “png”, “gif”, or “jpeg” formats, but must be named “png”, up to 320 pixels wide x 320 pixels tall, and in 24 bit color.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Entering no value for this parameter disables this feature. • The “image server uri” parameter supports FTP, HTTP, and HTTPS.
Format	Server URI String (image server uri: protocol://[username]:[password]@server)
Default Value	NA
Range	NA
Examples	<p>image server uri: http://mypictureserver.acme.com</p> <p>image server uri: ftp://mypictureserver.acme.com (anonymous ftp connection)</p> <p>image server uri: ftp://user:password@mypictureserver.acme.com (ftp connection using “user” and “password” for the credentials)</p>

BLF List URI Settings

Parameter– <i>list uri</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the URI that the BluStar 8000i uses to access the BLF list on the BroadSoft server when the BLF list key is pressed. When you specify a URI for this parameter, the BluStar 8000i uses the internet to access the BLF list on the BroadSoft server.
Format	sip:HTTP server path or Fully Qualified Domain Name
Default Value	NA
Range	NA
Example	list uri: sip:my8000i-blf-list@as.broadworks.com

BLF Subscription Period Settings

Parameter – <i>sip blf subscription period</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	The requested duration, in seconds, before the BLF subscription times out. The BluStar 8000i will attempt to re-subscribe to the BLF subscription service before the defined subscription period ends.
Format	Integer
Default Value	3600
Range	120 - 2147483647
Example	sip blf subscription period: 2000

Directed Call Pickup

Parameter – <i>directed call pickup</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Enables or disables the use of "directed call pickup" feature.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	directed call pickup: 1

Parameter – <i>directed call pickup prefix</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	<p>Allows you to enter a specific prefix string (depending on what is available on your server), that the BluStar 8000i automatically dials when dialing the Directed Call Pickup number.</p> <p>For example, for Broadsoft servers, you can enter a value of *97 for the "directed call pickup prefix". When the phone performs the Directed Call Pickup after pressing a BLF or BLF/List softkey, the phone prepends the *97 value to the designated extension of the BLF or BLF/List softkey when dialing out.</p> <p>Notes:</p> <ul style="list-style-type: none"> • The default method for the phone to use is Directed Call Pickup over BLF if the server provides applicable information. If the Directed Call Pickup over BLF information is missing in the messages to the server, the Directed Call Pickup by Prefix method is used if a value for the prefix code exists in the configuration. • You can define only one prefix at a time for the entire BLF/List. • The phone that picks up displays the prefix code + the extension number (for example, *981234 where prefix key = *97, extension = 1234). • Symbol characters are allowed (for example "*").
Format	Integer
Default Value	NA
Range	NA
Example	directed call pickup prefix: *97

XML Settings

Parameter – <i>xml get timeout</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Allows you to specify a timeout value, in seconds, that the BluStar 8000i waits for the far side to return a response after accepting the HTTP GET connection. If the far side accepts the GET connection but never returns a response, it blocks the BluStar 8000i until it is rebooted. If you enter a value greater than "0" for this parameter, the BluStar 8000i times out and will not be blocked.</p>
Format	Integer
Default Value	0 (never timeout)
Range	0 - 2147483647 seconds
Example	xml get timeout: 20

Advanced Operational Parameters

Update Caller ID Setting

Parameter – <i>sip update callerid</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables the updating of the Caller ID information during a call.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	sip update callerid: 1

Blind Transfer Setting

Parameter – <i>sip cancel after blind transfer</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Forces the BluStar 8000i to use the Blind Transfer method. This method sends the CANCEL message after the REFER message when blind transferring a call.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	sip cancel after blind transfer: 1

User-Agent Settings

Parameter – <i>sip user-agent</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Allows you to enable or disable the addition of the User-Agent and Server SIP headers in the SIP stack. The value of "0" prevents the UserAgent and Server SIP header from being added to the SIP stack. The value of "1" allows these headers to be added.
Format	Boolean
Default Value	1 (true)
Range	0-1 0 (false) 1 (true)
Example	sip user-agent: 0

Inactive Video Stream Settings

Parameter – <i>remove inactive video stream</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	When enabled, the BluStar 8000i will remove the video stream from the SDP in situations where the video stream should be disabled but the audio stream should be kept active.
Format	Boolean
Default Value	0
Range	0-1 0 (disabled) 1 (enabled)
Examples	remove inactive video stream: 1

Blacklist Duration Setting

Parameter – <i>sip blacklist duration</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the length of time, in seconds, that a failed server remains on the server blacklist. The BluStar 8000i avoids sending a SIP message to a failed server (if another server is available) for this amount of time. The value of "0" disables the blacklist feature.
Format	Integer
Default Value	300 (5 minutes)
Range	0 to 9999999
Example	sip blacklist duration: 600

Whitelist Proxy Setting

Parameter – <i>sip whitelist</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	This parameter enables/disables the whitelist proxy feature, as follows: Set to 0 to disable the feature. Set to 1 to enable the feature. When this feature is enabled, a BluStar 8000i accepts call requests from a trusted proxy server <i>only</i> . The BluStar 8000i rejects any call requests from an untrusted proxy server.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	sip whitelist: 1

XML SIP Notify Settings

Parameter – <i>sip xml notify event</i>	Configuration Files– aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Enables or disables the BluStar 8000i to accept or reject an aastra-xml SIP NOTIFY message.</p> <p>To ensure the SIP NOTIFY is coming from a trusted source, it is recommended that you enable the Whitelist Proxy Setting feature (“sip whitelist” parameter) on the BluStar 8000i. If enabled, and the BluStar 8000i receives a SIP NOTIFY from a server that is NOT on the whitelist (i.e. untrusted server), the BluStar 8000i rejects the message.</p>
Format	Boolean
Default Value	0
Range	0-1 0 (disabled) 1 (enabled)
Example	sip xml notify event: 1

Parameter – <i>action uri xml sip notify</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	<p>Specifies the URI to be called when an empty XML SIP NOTIFY is received by the BluStar 8000i. This parameter can use the following variable: \$\$LOCALIP\$\$</p> <p>The “sip xml notify event” parameter must be enabled.</p>
Format	HTTP(s) server path or Fully Qualified Domain Name
Default Value	NA
Range	NA
Example	action uri xml sip notify: http://myserver.com/myappli.xml

DNS Query Setting

Parameter– <i>sip dns query type</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the Domain Name Service (DNS) query method to use when the BluStar 8000i performs a DNS lookup.
Format	Integer
Default Value	1
Range	<p>0 A only - The BluStar 8000i issues requests for “A” (Host IP Address) records from the DNS server to get the IP address, and uses the default port number of 5060.</p> <p>1 SRV & A - The BluStar 8000i issues requests for “SRV” (Service Location Record) records from the DNS server to get the port number. Most often, the IP address is included in the response from the DNS server to avoid extra queries. If there is no IP address returned in the response, the BluStar 8000i sends out the request for “A” records from the DNS server to find the IP address.</p> <p>2 NAPTR & SRV & A - First, the BluStar 8000i sends “NAPTR” (Naming Authority Pointer) lookup to get the “SRV” pointer and service type. For example, if Global SIP transport protocol on the BluStar 8000i is “UDP”, and Proxy server on the BluStar 8000i is “test.aastra.com”, then:</p> <ol style="list-style-type: none"> 1. If the NAPTR record is returned empty, the BluStar 8000i will use the default value “_sip_udp.test.aastra.com” for the “SRV” lookup. 2. If the NAPTR record is returned “test.aastra.com SIP+D2U_sip_udp.abc.aastra.com”, the BluStar 8000i will use “_sip_udp.abc.aastra.com” for the “SRV” lookup. 3. If the NAPTR record is returned “test.aastra.com SIP+D2T_sip_tcp.test.aastra.com”, where the service type TCP mismatches the BluStar 8000i configured transport protocol “UDP”, the BluStar 8000i will ignore this value and use the default value “_sip_udp.test.aastra.com” for the “SRV” lookup. <p>Note: The BluStar 8000i does not use the service type sent by the NAPTR response to switch its transport protocol, nor does it use the NAPTR response to determine whether to use a secure or unsecure communication path. The BluStar 8000i will always use a global sip protocol that is configured on the BluStar 8000i via configuration files.</p> <p>After performing NAPTR, the BluStar 8000i sends “SRV” lookup to get the IP address and port number. If there is no IP address in the “SRV” response, then it sends out an “A” lookup to get it.</p>
Example	sip dns query type: 2

Ignore Out of Order SIP Requests

Parameter – <i>sip accept out of order requests</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables a workaround for non-compliant SIP devices (for example, Asterisk) that do not increment the CSeq numbers in SIP requests sent to the BluStar 8000i.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	sip accept out of order requests: 1

Optional “Allow” and “Allow-Event” Headers

Parameter – <i>sip notify opt headers</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables and disables whether or not the “Allow” and “Allow-Events” optional headers are included in the SIP NOTIFY messages sent from the BluStar 8000i to the server.
Format	Boolean
Default Value	1
Range	0-1 0 (disabled - optional headers are removed from the SIP NOTIFY message) 1 (enabled - no change; optional headers are included in SIP NOTIFY message)
Example	sip notify opt headers: 0

P-Asserted Identity (PAI)

Parameter – <i>sip pai</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables whether the SIP PAI displays on the BluStar 8000i.
Format	Boolean
Default Value	1
Range	0-1 0 (disabled) 1 (enabled)
Example	sip pai: 0

Compact SIP Header

Parameter – <i>sip compact headers</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Enables or disables the BluStar 8000i to use compact SIP headers in the SIP packets sent from the BluStar 8000i.
Format	Boolean
Default Value	0 (disabled- uses long SIP header format)
Range	0-1 0 (disabled- uses long SIP header format) 1 (enabled- uses short (compact) SIP header format)
Example	sip compact headers: 1

Dial Plan Terminator

Parameter – <i>sip dial plan terminator</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	Specifies whether or not the hash/pound (i.e. "#") key should be used as a dial pad terminator. When disabled (default), the hash/pound key, while performing an outgoing call on an open line, acts as a dial plan terminator (i.e. dials out the call immediately). When enabled, the hash/pound key does not act as a dial plan terminator and is instead sent as %23.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	sip dial plan terminator: 1

Troubleshooting Parameters

The following parameters in this section allow the system administrator to set alert and logging settings for troubleshooting purposes.

On-Screen Connection Quality Alarms

Parameter – <i>packet loss lower threshold</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the lower threshold of packet loss whereby if the percentage of packet loss is above the configured threshold, the poor network performance alert will be displayed on screen.
Format	Percentage
Default Value	8
Range	0-100
Example	packet loss lower threshold: 6

Parameter – <i>packet loss upper threshold</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the upper threshold of packet loss whereby if the percentage of packet loss is above the configured threshold, the very poor network performance alert will be displayed on screen.
Format	Percentage
Default Value	15
Range	0-100
Example	packet loss upper threshold: 20

Syslog Settings

Note:

Some parameters in this section utilize a different syntax and must be prefaced by the term “BluStar Settings:”. Such parameters can be recognized by their respective examples.

Syslog Location

Parameter – <i>log server ip</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the log server IP address for which to save system log files for troubleshooting purposes.
Format	IP address
Default Value	0.0.0.0
Range	NA
Example	log server ip: 192.168.3.2

Parameter – <i>log server port</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	Specifies the log server IP port to use to save log files for troubleshooting purposes.
Format	Integer
Default Value	514
Range	Any valid IP port
Example	log server port: 514

System-Wide Logging

Parameter – <i>LogLevel</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg																						
Description	Sets the baseline log level for all of the modules. Individual modules will use the higher of this parameter or their own specific setting. There are 10 base line log levels for the modules. Note: Setting a log level higher than 4 may impact performance.																						
Format	Integer																						
Default Value	1 (Fatal Error)																						
Range	<table> <tr> <th>#</th><th>Log Level</th></tr> <tr> <td>0</td><td>Always</td></tr> <tr> <td>1</td><td>Fatal Error</td></tr> <tr> <td>2</td><td>Serious Error</td></tr> <tr> <td>3</td><td>Minor Error</td></tr> <tr> <td>4</td><td>Warning</td></tr> <tr> <td>5</td><td>Info</td></tr> <tr> <td>6</td><td>Verbose</td></tr> <tr> <td>7</td><td>Debug Level 1</td></tr> <tr> <td>8</td><td>Debug Level 2</td></tr> <tr> <td>9</td><td>Debug Level 3</td></tr> </table>	#	Log Level	0	Always	1	Fatal Error	2	Serious Error	3	Minor Error	4	Warning	5	Info	6	Verbose	7	Debug Level 1	8	Debug Level 2	9	Debug Level 3
#	Log Level																						
0	Always																						
1	Fatal Error																						
2	Serious Error																						
3	Minor Error																						
4	Warning																						
5	Info																						
6	Verbose																						
7	Debug Level 1																						
8	Debug Level 2																						
9	Debug Level 3																						
Example	BluStar Settings: LogLevel=2																						

Parameter – <i>WriteToFlag</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	A mask that controls the data path(s) for the logging data.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	BluStar Settings: WriteToFlag=0

SIP Stack Logging

Parameter – <i>VSipServer_LogLevel</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg																		
Description	Sets the SIP stack log level. There are 8 SIP stack log levels.																		
Format	Integer																		
Default Value	3 (Minor Error)																		
Range	<table> <tr> <th>#</th><th>Log Level</th></tr> <tr> <td>0</td><td>Always</td></tr> <tr> <td>1</td><td>Fatal Error</td></tr> <tr> <td>2</td><td>Serious Error</td></tr> <tr> <td>3</td><td>Minor Error</td></tr> <tr> <td>4</td><td>Warning</td></tr> <tr> <td>5</td><td>Info</td></tr> <tr> <td>6</td><td>Verbose</td></tr> <tr> <td>7</td><td>Debug Level 1</td></tr> </table>	#	Log Level	0	Always	1	Fatal Error	2	Serious Error	3	Minor Error	4	Warning	5	Info	6	Verbose	7	Debug Level 1
#	Log Level																		
0	Always																		
1	Fatal Error																		
2	Serious Error																		
3	Minor Error																		
4	Warning																		
5	Info																		
6	Verbose																		
7	Debug Level 1																		
Example	BluStar Settings: VSipServer_LogLevel=5																		

Parameter – <i>VSipServer_WriteToFlag</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	A mask that controls the data path(s) for the SIP stack logging data.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	BluStar Settings: VSipServer_WriteToFlag=1

Debug Logging

Parameter – <i>DBG_Modules</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg																																				
Description	Allows for enhanced severity filtering of log calls for specific debug modules.																																				
Format	String, list of module names separated by a comma.																																				
Default Value	NA																																				
Range	<table> <tr> <th>Debug Modules</th><th>Description</th></tr> <tr> <td>APPE</td><td>GUI appearance, line manager functionality</td></tr> <tr> <td>AURL</td><td>curl IPC debugging</td></tr> <tr> <td>CALL</td><td>trace ViPrCall class</td></tr> <tr> <td>CERT</td><td>curl IPC debugging, SSL errors</td></tr> <tr> <td>CONT</td><td>IPC contacts</td></tr> <tr> <td>DIRC</td><td>IPC directory debugging</td></tr> <tr> <td>FOLD</td><td>debugging AB folder (base class for personal and global folders, contacts and directory)</td></tr> <tr> <td>IPCD</td><td>IPC debugging</td></tr> <tr> <td>NOTI</td><td>IPC notifications debugging</td></tr> <tr> <td>PRES</td><td>IPC presence debugging</td></tr> <tr> <td>PROF</td><td>curl IPC debugging, profiling</td></tr> <tr> <td>SESN</td><td>curl IPC session debugging</td></tr> <tr> <td>SETS</td><td>curl IPC settings debugging</td></tr> <tr> <td>SETU</td><td>user settings debugging</td></tr> <tr> <td>STUB</td><td>stub debugging</td></tr> <tr> <td>SWUD</td><td>auto update class</td></tr> <tr> <td>TOOL</td><td>debug settings screen</td></tr> </table>	Debug Modules	Description	APPE	GUI appearance, line manager functionality	AURL	curl IPC debugging	CALL	trace ViPrCall class	CERT	curl IPC debugging, SSL errors	CONT	IPC contacts	DIRC	IPC directory debugging	FOLD	debugging AB folder (base class for personal and global folders, contacts and directory)	IPCD	IPC debugging	NOTI	IPC notifications debugging	PRES	IPC presence debugging	PROF	curl IPC debugging, profiling	SESN	curl IPC session debugging	SETS	curl IPC settings debugging	SETU	user settings debugging	STUB	stub debugging	SWUD	auto update class	TOOL	debug settings screen
Debug Modules	Description																																				
APPE	GUI appearance, line manager functionality																																				
AURL	curl IPC debugging																																				
CALL	trace ViPrCall class																																				
CERT	curl IPC debugging, SSL errors																																				
CONT	IPC contacts																																				
DIRC	IPC directory debugging																																				
FOLD	debugging AB folder (base class for personal and global folders, contacts and directory)																																				
IPCD	IPC debugging																																				
NOTI	IPC notifications debugging																																				
PRES	IPC presence debugging																																				
PROF	curl IPC debugging, profiling																																				
SESN	curl IPC session debugging																																				
SETS	curl IPC settings debugging																																				
SETU	user settings debugging																																				
STUB	stub debugging																																				
SWUD	auto update class																																				
TOOL	debug settings screen																																				
Example	BluStar Settings: DBG_Modules=SESN, CALL																																				

Parameter – <i>DBG_LogLevel</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg																						
Description	Sets the debug log level. There are 10 debug log levels for the modules. Note: The debug log level must be less than or equal to the system-wide log level for the debug module logging to output.																						
Format	Integer																						
Default Value	1 (Fatal Error)																						
Range	<table> <tr> <th>#</th><th>Log Level</th></tr> <tr> <td>0</td><td>Always</td></tr> <tr> <td>1</td><td>Fatal Error</td></tr> <tr> <td>2</td><td>Serious Error</td></tr> <tr> <td>3</td><td>Minor Error</td></tr> <tr> <td>4</td><td>Warning</td></tr> <tr> <td>5</td><td>Info</td></tr> <tr> <td>6</td><td>Verbose</td></tr> <tr> <td>7</td><td>Debug Level 1</td></tr> <tr> <td>8</td><td>Debug Level 2</td></tr> <tr> <td>9</td><td>Debug Level 3</td></tr> </table>	#	Log Level	0	Always	1	Fatal Error	2	Serious Error	3	Minor Error	4	Warning	5	Info	6	Verbose	7	Debug Level 1	8	Debug Level 2	9	Debug Level 3
#	Log Level																						
0	Always																						
1	Fatal Error																						
2	Serious Error																						
3	Minor Error																						
4	Warning																						
5	Info																						
6	Verbose																						
7	Debug Level 1																						
8	Debug Level 2																						
9	Debug Level 3																						
Example	BluStar Settings: DBG_LogLevel=2																						

Parameter – <i>DBG_WriteToFlag</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg
Description	A mask that controls the data path(s) for the debug logging data.
Format	Boolean
Default Value	0 (disabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	BluStar Settings: DBG_WriteToFlag=1

Feedback Application Settings

Parameter – <i>enable user feedback</i>	Configuration Files – aastra.cfg, <model>.cfg, <mac>.cfg, <user>.cfg
Description	This administrator parameter enables or disables the feedback application located in the apps menu on the BluStar 8000i.
Format	Boolean
Default Value	1 (enabled)
Range	0-1 0 (disabled) 1 (enabled)
Example	enable user feedback: 0

Appendix B

Sample Configuration Files

This section consists of the sample configuration files necessary to configure the BluStar. The general format is similar to the configuration files used by several Unix-based programs. Any text following a number sign (#) on a line is considered to be a comment, unless the # is contained within double-quotes. Currently, Boolean fields use "0" for false and "1" for true.

Aastra.cfg

aastra.cfg

```
language name: French
time zone name: us-eastern
```

<model>.cfg

8000i.cfg

```
pbx mode:1
user config URL: http://configserver1/aastracfg
```

<Mac>.cfg

00085D112233.cfg

```
update url: HTTP://configserver1/aastracfg
```

<user>.cfg

jdoe.cfg

```
directory 1:ftp://configserver1/usercfg/global.csv
directory 2:ftp://configserver1/usercfg/30401.csv
sip auth name:30401
sip display name:John Doe
sip password:30401
sip proxy ip:10.55.102.190
sip proxy port:5060
sip registrar ip:10.55.102.190
sip registrar port:5060
sip screen name:John Doe
sip screen name 2:30401
sip user name:30401
```

Appendix C

OpenVPN Configuration

This example is applicable for an OpenVPN implementation using Fedora 13. The commands or file locations will be different depending on the respective OS or Linux distribution being employed. IPs and directories in the following examples should be changed to suit your own needs.

Note:

For further information on how to configure OpenVPN to your specific needs, please refer to the [OpenVPN HOWTO website](#).

Server Requirements

The basic requirements for implementing OpenVPN include the following:

- Physical server (with Fedora 13 installed) for use as the OpenVPN and Apache HTTP server:
 - OpenVPN requirements:
 - Two ethernet cards (eth0 and eth1)
 - Utilizing the UDP protocol
 - Utilizing the default port of 1194
 - Apache HTTP requirements:
 - Utilizing the TCP protocol
 - Utilizing the default port of 443
- Optional - DHCP server (for client IP address configuration)
- Optional - Internal DNS server (for resolving internal FQDNs to internal IPs)
- Optional - Public DNS server (for resolving public FQDNs to external IPs)

Note:

It is recommended that the server utilize Gigabit Ethernet network interfaces for better performance.

Physical Server and Network Environment

The following procedure details what steps are needed to configure OpenVPN with regards to the physical server and the corporate network:

1. Install Fedora 13 on the physical server to be used as the OpenVPN and Apache HTTP server.
2. Configure eth0 and eth1 with the respective IP addresses and the desired domain names.
For example, eth0 - 10.1.1.20 and eth1 - 10.1.1.21.
3. Configure the server to listen on port 443 (for Apache HTTP use).
4. For security purposes, disable the listing directory function enabled by Apache by default. To disable the function:
 - a) Open httpd.conf:
 - # vi /etc/httpd/conf/httpd.conf
 - b) Find "<Directory "/var/www/html">" and change "Options Indexes FollowSymLinks" to "Options FollowSymLinks".
 - c) Perform a graceful restart:
 - # apachectl graceful

5. Configure forwarding rules for the corporate firewall:
 - For OpenVPN use forward the external IP address, protocol, and port to the eth1 IP, protocol, and port.
For example, 200.100.100.245, udp/1194 to 10.1.1.21, udp/1194.
 - For Apache HTTP use forward the external IP address, protocol, and port to the eth1 IP, protocol, and port.
For example, 200.100.100.245, tcp/443 to 10.1.1.21, tcp/443.
6. Configure the server to ensure the vpnclient directory (e.g. /opt/BluStar/www/html/vpnclient) is accessible from https://external ip address/vpnclient/ (e.g. https://200.100.100.245/vpnclient).

Note:

This directory will contain tarballs for remote terminals.

Configuration Files/Scripts and Certificates/Keys

The following tables detail the configuration files/scripts and generated certificates/keys needed for both the server and client for this particular example.

Server-Side Files	Description
Configuration Files and Scripts	
server.conf	General server configuration file to configure local eth1 IP, listening port, udp protocol, etc.
bridge-start bridge-stop	Linux scripts to start and stop ethernet bridging.
iptables.txt	File containing the iptable rules allowing for packets to flow freely between clients and server.
Generated Certificates/Keys	
ca.crt ca.key	SSL/TLS root CA certificate and root CA key. Note: The server and clients will share the same ca.crt file.
server.key server.crt	Server certificate and server key.
dh1024.pem (server only)	Diffie Hellman parameters.
ta.key	HMAC firewall key to help block DDoS attacks and UDP port flooding. Note: The server and client will share the same ta.key file.
Client-Side Files	
Configuration Files and Scripts	
client.conf	General client configuration file to configure remote FQDN/IP, listening port, udp protocol, etc.
up.sh down.sh dhclient-tap0.tpl dhclient-tap0.sh	Linux scripts for DHCP-related tasks.
Generated Certificates/Keys	
ca.crt	SSL/TLS root CA certificate. Note: The server and clients will share the same ca.crt file.
client.key client.crt	Client certificate and client key.
ta.key	HMAC firewall key to help block DDoS attacks and UDP port flooding. Note: The server and client will share the same ta.key file.

Creating the Server-Side Sample Configuration Files/Scripts

The following server-side sample configuration files/scripts are required for this example and can be used as a guideline when configuring OpenVPN for your network. Cut and paste the applicable lines of code into the text editor of your choice and save the file using the respective filename.

Note:

All server-side sample configuration files/scripts for this example should be placed in the `/etc/openvpn` directory.

Sample server.conf

```
local 10.1.1.21
port 1194
proto udp
dev tap0
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server-bridge
client-to-client
duplicate-cn
keepalive 10 120
tls-auth ta.key 0
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 4
mute 20
tun-mtu 1500
mssfix
fragment 1300
log /var/log/openvpn.log
```

Note:

For detailed functional descriptions of the above server.conf parameters, please refer to the [OpenVPN HOWTO website](#).

Sample bridge-start

```
#!/bin/bash

#####
# Set up Ethernet bridge on Linux
# Requires: bridge-utils
#####

# Define Bridge Interface
br="br0"

# Define list of TAP interfaces to be bridged,
# for example tap="tap0 tap1 tap2".
tap="tap0"

# Define physical ethernet interface to be bridged
# with TAP interface(s) above.
eth="eth1"
eth_ip="10.1.1.21"
eth_netmask="255.255.255.0"
eth_broadcast="10.1.1.255"

for t in $tap; do
    openvpn --mktun --dev $t
done

brctl addbr $br
brctl addif $br $eth

for t in $tap; do
    brctl addif $br $t
done

for t in $tap; do
    ifconfig $t 0.0.0.0 promisc up
done

ifconfig $eth 0.0.0.0 promisc up

ifconfig $br $eth_ip netmask $eth_netmask broadcast $eth_broadcast
```

Sample bridge-stop

```
#!/bin/bash

#####
# Tear Down Ethernet bridge on Linux
#####

# Define Bridge Interface
br="br0"

# Define list of TAP interfaces to be bridged together
tap="tap0"

ifconfig $br down
brctl delbr $br

for t in $tap; do
    openvpn --rmtun --dev $t
done
```

Sample iptables.txt

```
iptables -I INPUT -i tap0 -j ACCEPT
iptables -I INPUT -i br0 -j ACCEPT
iptables -I FORWARD -i br0 -j ACCEPT
iptables -I INPUT -p tcp -m tcp --dport 1194 --tcp-flags FIN,SYN,RST,ACK SYN -j
ACCEPT
iptables -I INPUT -p udp -m udp --dport 1194 -j ACCEPT
#iptables -I FORWARD -m physdev --physdev-in tap0 -j DROP
#iptables -I FORWARD -m physdev --physdev-in tap0 -m mac --mac-source
70:71:BC:88:12:7D -j ACCEPT
```

Note:

The following lines of code will be separated onto two lines when cut and pasted into your text editor:

```
#iptables -I FORWARD -m physdev --physdev-in tap0 -m mac --mac-source
70:71:BC:88:12:7D -j ACCEPT
```

The above lines are in fact one line and should be merged together manually in your text editor.

Installing the OpenVPN Server and Creating Certificates/Keys

When the above server-side configuration files/scripts have been created, enter the following commands to install the OpenVPN server and create the necessary certificates/keys and directories:

```
# yum install openvpn bridge-utils

# cd /usr/share/openvpn/easy-rsa/2.0
# . ./vars
# ./clean-all
# ./build-ca
# ./build-dh
# ./build-key-server server
# ./build-key client
# /usr/sbin/openvpn --genkey --secret keys/ta.key

# cd keys
# cp ca.crt ca.key server.key server.crt dh1024.pem ta.key /etc/openvpn

# mkdir -p /opt/BluStar/www/html/vpnclient/client
# cp ca.crt client.key client.crt ta.key /opt/BluStar/www/html/vpnclient/client
# ln -snf /opt/BluStar/www/html/vpnclient/ /var/www/html/
```

Note:

After the following commands are executed you will be asked to additional information such as city, organization, etc.:

```
#!/build-ca
#!/build-key-server server
#!/build-key client
```

Specific values can be entered, or the default can be selected by simply pressing the Enter key.

Creating the Client-Side Sample Configuration Files/Scripts

The following client-side sample configuration files/scripts are required for this example and can be used as a guideline when configuring OpenVPN for your network. Cut and paste the applicable lines of code into the text editor of your choice and save the file using the respective filename.

Note:

All client-side sample configuration files/scripts for this example should be placed in the /opt/BluStar/www/html/vpnclient/client directory.

Sample client.conf

```
client
dev tap0
proto udp
remote 200.100.100.245 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
ns-cert-type server
tls-auth ta.key 1
comp-lzo
verb 3
mute 1
script-security 2
up "./up.sh"
down "./down.sh"
log /var/log/openvpn.log
tun-mtu 1500
mssfix
fragment 1300
```

Note:

For detailed functional descriptions of the above client.conf parameters, please refer to the [OpenVPN HOWTO website](#).

Sample up.sh

```
#!/bin/sh
echo `date`: VPN channel is up! param: $@
/etc/openvpn/dhclient-tap0.sh up 2>&1 &
```

Sample down.sh

```
#!/bin/sh
echo `date`: VPN channel is down! param: $@
/etc/openvpn/dhclient-tap0.sh down 2>&1 &
```

Sample dhclient-tap0.tpl

```
send dhcp-parameter-request-list 1,2,3,6,7,12,15,28,40,41,42,43,66,159,160;
send vendor-class-identifier "AastraBluStar8000i-vpn";
send host-name "BluStarHost-tap0";
```

Sample dhclient-tap0.sh

```
#!/bin/sh
CONFDIR=/etc/openvpn
DHDIR=/var/lib/dhclient
case "$1" in
    up)
kill -9 `cat $DHDIR/dhclient-tap0.pid`
sleep 3
eth0mac=`/sbin/ifconfig eth0|grep eth0|awk '{print $5}'`
echo `date`: set tap0 mac as $eth0mac
/sbin/ip link set dev tap0 address $eth0mac
/sbin/ifconfig tap0 0.0.0.0 up
route=`/sbin/route -n|grep ^0.0.0.0|awk '{print $2}'`
echo `date`: trying to run dhcp for tap0. default gw:$route
cat $CONFDIR/dhclient-tap0.tpl > $DHDIR/dhclient-tap0.conf
rm -f $DHDIR/dhclient-tap0.leases
serverip=`cat $CONFDIR/client.conf|grep ^remote|awk '{print $2}'`
echo `date`: trying to reserve route for server:$serverip
/sbin/route add -host $serverip gw $route
/sbin/dhclient -1 -q -cf $DHDIR/dhclient-tap0.conf -lf $DHDIR/dhclient-
tap0.leases -pf $DHDIR/dhclient-tap0.pid tap0
;;
    down)
target=`/sbin/route|grep UGH|head -1|awk '{print $1}'`
route=`/sbin/route|grep UGH|head -1|awk '{print $2}'`
echo `date`: trying to take down tap0. default gw:$route
/sbin/route del $target
/sbin/route add default gw $route
kill -9 `cat $DHDIR/dhclient-tap0.pid`
rm -f $DHDIR/dhclient-tap0.leases
# restore predhclient config
cd $DHDIR
for file in *.predhclient.tap0; do
    echo cp -f $file /etc/${file%.predhclient.tap0}
    cp -f $file /etc/${file%.predhclient.tap0}
done
;;
*)
    echo "$0 up|down"
;;
esac
exit 0
```

Note:

The following lines of code will be separated onto two lines when cut and pasted into your text editor:

```
/sbin/dhclient -l -q -cf $DHDIR/dhclient-tap0.conf -lf $DHDIR/dhclient-  
tap0.leases -pf $DHDIR/dhclient-tap0.pid tap0
```

The above lines are in fact one line and should be merged together manually in your text editor.

Preparing the Ethernet Bridge and Firewall Rules

Before executing the ethernet bridge, ensure (for this particular example) the server configuration files/scripts are located in /etc/openvpn/ and the client configuration files/scripts are located in opt/BluStar/www/html/vpnclient/client/.

Enter the following commands to prepare the ethernet bridge and firewall rules:

```
# cd /etc/openvpn  
# vi server.conf
```

Note:

Ensure the "local x.x.x.x" parameter is configured properly as per your server's local IP.

```
# vi bridge-start
```

Note:

Ensure the following parameters are configured properly as per your server network interface's settings:

- eth
- eth_ip
- eth_netmask
- eth_broadcast

```
# sh ./bridge-start  
# vi iptables.txt
```

Note:

For enhanced security, the last two lines in iptables.txt can be uncommented and the MAC address can be configured to only allow internal network access to specific terminals.

```
# sh iptables.txt
```

Note:

For more information about the above commands and ethernet bridging, please refer to the [OpenVPN Ethernet Bridging website](#).

Starting the OpenVPN Service

Enter the following command to start the OpenVPN service.

```
# service openvpn start
```

When the service has started, typing `ifconfig` should reveal details for `br0`, `eth0`, `eth1`, `lo`, and `tap0`.

In this example, the `openvpn.log` file in the `/var/log/` directory can be viewed for errors.

Preparing the Configuration Tarball for Remote Terminals

Enter the following commands to prepare the configuration tarball for remote terminals:

```
# cd /opt/BluStar/www/html/vpnclient/client
# vi client.conf
```

Note:

Ensure the “remote x.x.x.x 1194” parameter is configured properly as per your external IP to internal IP mapping and port on the server. It is recommended to use the IP address if issues occur when using the FQDN.

```
# chmod 755 *.sh
# cd ..
# tar zcvf client.tgz client
```

For security purposes, it is recommended that the resulting `client.tgz` file be renamed to something random. Enter the following commands to rename the file (“client-8X5D8WE23” can be replaced with any unique filename):

```
# mv client client-8X5D8WE23
# tar zcvf client-8X5D8WE23.tgz client-8X5D8WE23
```

After creating the configuration tarball, open a browser window on your PC and try to download the newly created tarball from the configured URI (e.g. <https://200.100.100.245/vpnclient/client-8X5D8WE23.tgz>)

If any errors occur, ensure the Apache HTTP server settings, external firewall mappings, and/or iptables settings are configured correctly.

Configuring the BluStar 8000i Terminal to Enable VPN

To configure the BluStar 8000i terminal to enable VPN:

The screenshot shows the 'terminal identity' configuration screen. At the top, there is a navigation bar with icons for 'user identity', 'sounds', 'call handling', 'terminal identity' (highlighted with a green box), 'utilities', 'fingerprint', 'contacts', 'LDAP directory', and a 'back' button with a green checkmark. The main area is divided into three sections: 'call server', 'network settings', and 'VPN'. In the 'call server' section, 'server type' has two buttons: 'BluStar Application Server' and 'SIP Call Server' (highlighted with a green box). Below it, 'configuration server' has a text field 'enter Configuration Server URL'. In the 'network settings' section, there are checkboxes for 'use IPv6' and 'disable autonegotiate', and a text field for 'MTU' with the value '1500'. In the 'VPN' section, there is a checkbox for 'use VPN' which is checked with a green box, and a text field for 'certificate location' containing a series of asterisks and a close button. To the right of the 'VPN' section, there is a 'VLAN' section with checkboxes for 'use VLAN' and a text field for 'VLAN id' with the value '1'.

1. On the respective BluStar 8000i terminal, touch **app menu** > **tools** > **terminal identity** > **advanced**.
2. Under **VPN** enter the location of the client tarball file in the **certificate location** field.
3. Touch **use VPN** to enable the VPN client.
4. Touch the **back** button to return to the main terminal identity screen.
5. Touch **done** and then **Restart** to restart the BluStar 8000i terminal and allow the changes to take effect.

Limited Warranty

(Not applicable in Australia – see below for Limited Warranty in Australia)

Aastra warrants this product against defects and malfunctions in accordance with Aastra's authorized, written functional specification relating to such products during a one (1) year period from the date of original purchase ("Warranty Period"). If there is a defect or malfunction, Aastra shall, at its option, and as the exclusive remedy, either repair or replace the product at no charge, if returned within the Warranty Period. If replacement parts are used in making repairs, these parts may be refurbished, or may contain refurbished materials. If it is necessary to replace the product, it may be replaced with a refurbished product of the same design and color. If it should become necessary to repair or replace a defective or malfunctioning product under this warranty, the provisions of this warranty shall apply to the repaired or replaced product until the expiration of ninety (90) days from the date of pick up, or the date of shipment to you, of the repaired or replacement product, or until the end of the original Warranty Period, whichever is later. Proof of the original purchase date is to be provided with all products returned for warranty repairs.

Exclusions

Aastra does not warrant its products to be compatible with the equipment of any particular telephone company. This warranty does not extend to damage to products resulting from improper installation or operation, alteration, accident, neglect, abuse, misuse, fire or natural causes such as storms or floods, after the product is in your possession. Aastra will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use.

Aastra shall not be liable for any incidental or consequential damages, including, but not limited to, loss, damage or expense directly or indirectly arising from the customer's use of or inability to use this product, either separately or in combination with other equipment. This paragraph, however, shall not apply to consequential damages for injury to the person in the case of products used or bought for use primarily for personal, family or household purposes.

This warranty sets forth the entire liability and obligations of Aastra with respect to breach of warranty, and the warranties set forth or limited herein are the sole warranties and are in lieu of all other warranties, expressed or implied, including warranties or fitness for particular purpose and merchantability.

Warranty Repair Services

Should the product fail during the Warranty Period;

- **In North America**, please call 1-800-574-1611 for further information.
- **Outside North America**, contact your sales representative for return instructions.

You will be responsible for shipping charges, if any. When you return this product for warranty service, you must present proof of purchase.

After Warranty Service

Aastra offers ongoing repair and support for this product. This service provides repair or replacement of your Aastra product, at Aastra's option, for a fixed charge. You are responsible for all shipping charges. For further information and shipping instructions:

- **In North America**, contact our service information number: 1-800-574-1611.
- **Outside North America**, contact your sales representative.

Note:

Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. This restriction applies during and after the Warranty Period. Unauthorized repair will void the warranty.

Limited Warranty (Australia Only)

The benefits under the Aastra Limited Warranty below are in addition to other rights and remedies to which you may be entitled under a law in relation to the products.

In addition to all rights and remedies to which you may be entitled under the *Competition and Consumer Act 2010* (Commonwealth) and any other relevant legislation, Aastra warrants this product against defects and malfunctions in accordance with Aastra's authorized, written functional specification relating to such products during a one (1) year period from the date of original purchase ("Warranty Period"). If there is a defect or malfunction, Aastra shall, at its option, and as the exclusive remedy under this limited warranty, either repair or replace the product at no charge, if returned within the Warranty Period.

Repair Notice

To the extent that the product contains user-generated data, you should be aware that repair of the goods may result in loss of the data. Goods presented for repair may be replaced by refurbished goods of the same type rather than being repaired. Refurbished parts may be used to repair the goods. If it is necessary to replace the product under this limited warranty, it may be replaced with a refurbished product of the same design and color.

If it should become necessary to repair or replace a defective or malfunctioning product under this warranty, the provisions of this warranty shall apply to the repaired or replaced product until the expiration of ninety (90) days from the date of pick up, or the date of shipment to you, of the repaired or replacement product, or until the end of the original Warranty Period, whichever is later. Proof of the original purchase date is to be provided with all products returned for warranty repairs.

Exclusions

Aastra does not warrant its products to be compatible with the equipment of any particular telephone company. This warranty does not extend to damage to products resulting from improper installation or operation, alteration, accident, neglect, abuse, misuse, fire or natural causes such as storms or floods, after the product is in your possession. Aastra will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use.

To the extent permitted by law, Aastra shall not be liable for any incidental damages, including, but not limited to, loss, damage or expense directly or indirectly arising from your use of or inability to use this product, either separately or in combination with other equipment. This paragraph, however, is not intended to have the effect of excluding, restricting or modifying the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (**the ACL**), the exercise of a right conferred by such a provision or any liability of Aastra in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

This express warranty sets forth the entire liability and obligations of Aastra with respect to breach of this express warranty and is in lieu of all other express or implied warranties other than those conferred by a law whose application cannot be excluded, restricted or modified. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Warranty Repair Services

Procedure: Should the product fail during the Warranty Period and you wish to make a claim under this express warranty, please contact the Aastra authorized reseller who sold you this product (details as per the invoice) and present proof of purchase. You will be responsible for shipping charges, if any.

Manufacturer: Aastra Telecom Australia Pty Ltd
745 Springvale Road
Mulgrave VIC 3170
ABN 16 140 787 195
Phone: +61 3 8562 2700

Limitation of Liability for Products not of a kind ordinarily acquired for personal, domestic or household use or consumption (e.g. goods/services ordinarily supplied for business-use)

- 1.1** To the extent permitted by law and subject to clause 1.2 below, the liability of Aastra to you for any non-compliance with a statutory guarantee or loss or damage arising out of or in connection with the supply of goods or services (whether for tort (including negligence), statute, custom, law or on any other basis) is limited to:
- a)** in the case of services:
 - i)** the resupply of the services; or
 - ii)** the payment of the cost of resupply; and
 - b)** in the case of goods:
 - i)** the replacement of the goods or the supply of equivalent goods; or
 - ii)** the repair of the goods; or
 - iii)** the payment of the cost of replacing the goods or of acquiring equivalent goods; or
 - iv)** the payment of the cost of having the goods repaired.
- 1.2** Clause 1.1 is not intended to have the effect of excluding, restricting or modifying:
- a)** the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (**the ACL**); or
 - b)** the exercise of a right conferred by such a provision; or
 - c)** any liability of Aastra in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

After Warranty Service

Aastra offers ongoing repair and support for this product. If you are not otherwise entitled to a remedy for a failure to comply with a guarantee that cannot be excluded under the Australian Consumer Law, this service provides repair or replacement of your Aastra product, at Aastra's option, for a fixed charge. You are responsible for all shipping charges. For further information and shipping instructions contact:

Aastra Telecom Australia Pty Ltd
745 Springvale Road
Mulgrave VIC 3170
ABN 16 140 787 195
Phone: +61 3 8562 2700

Note:

Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. Unauthorized repair will void this express warranty.

Index

A

audio/video	1-8
auto-answer	A-68
auto-resync	2-13

B

blacklist duration	5-3
blind transfer, SIP message sequence	5-2
BluStar Application Server	Preface-i
busy lamp field (BLF)	4-37

C

call	
appearance	1-23
forward	4-12
history	4-13
screen	1-23
caller ID	5-1
configuration files	2-1
installing	2-3
precedence	2-2
sample	B-1
configuration server	1-26
configuring	2-13
download precedence	3-1, 3-6
protocol	2-10
settings	2-10
contacts	4-18

D

default gateway	3-2
DHCP	1-25, 3-1–3-11
enable/disable	3-3
Option 12 Hostname	3-4
Option 77 User Class	3-5
Options 159 and 160	3-5
Options 66	3-3
dial plan, emergency dial plan and pattern matching	4-35
DiffServ QoS	3-8
directory	4-16
diversion display	4-40
DNS	
DNS A records	2-13
DNS caching	3-6
DNS1	3-2
DNS2	3-2
queries, configurable	5-5

E

encryption	
methods for	2-4
procedure for	2-8

F

factory defaults	4-3
fingerprint reader	1-12

H

hardware features	1-2
-------------------------	-----

headers

allow and allow-event	5-7
compact SIP	5-8
useragent and server SIP	5-2

I

Installation	
considerations	1-25

K

key descriptions	1-4
------------------------	-----

L

LDAP settings	4-24
LDAP base DN	4-25
LDAP name	4-24
LDAP server	4-24
user defined LDAP	4-25
locale settings	4-10

M

MAC address in REGISTER messages	5-2
Microsoft Exchange contacts	4-30
missed calls indicator	4-15

N

network settings	3-1
configuring manually	3-6
network time protocol	3-8

O

out of sequence errors	5-6
out-of-band DTMF	3-13

P

parameters	
advanced SIP	A-25
audio/video settings	A-63
blacklist duration	A-79
BLF list URI	A-75
BLF subscription period	A-76
blind transfer setting	A-78
call forward settings	A-65
call history settings	A-30
compact SIP header	A-83
configuration server settings	A-11
DHCP option settings	A-10
directed call pickup	A-76
directory settings	A-28
dns query setting	A-81
DSCP	A-8
DTMF settings	A-56
emergency dial plan	A-70
LDAP settings	A-30, A-32
local settings	A-60
MAC Address/Line Number	A-26
Microsoft Exchange contacts	A-44
missed calls indicator settings	A-30
network	A-4
out of order SIP requests	A-82

Picture ID feature	A-75
rport	A-20
screen settings	A-58
sip notify opt headers	A-82
sip pai	A-82
SIP route header	A-83
SIP settings	A-20
terminal security settings	A-56
ToS	A-8
updating caller ID	A-78
user settings	A-49
user-agent settings	A-78
VLAN	A-8
whitelist proxy	A-79
XML settings	A-77
XML SIP notify	A-80
parameters, list of configurable	A-4, A-84
parameters, setting in configuration files	A-3
P-Asserted Identity (PAI)	5-7
password	1-11, 4-8
picture ID	4-36
play warning tone	4-13
Q	
QoS	3-8
R	
real-time transport protocol (RTP)	3-14
requirements, IP phone	1-25
S	
safety	Preface-ii
screen settings	4-10
security	1-23
security settings	
terminal	4-8
self view	1-8
SIP	
basic settings	3-11
subnet mask	3-1
system mointor	6-1
system overview	1-1
T	
terminal identity	4-2
time server	3-2
ToS	3-8
touch screen basics	
call screen	1-23
home screen	1-17
lock screen	1-23
U	
Upgrade	Preface-i
User config file upload	4-8
username	1-11, 1-24, 4-8, A-21, A-71
V	
VLAN	
DSCP Range	3-8
priority mapping	3-8
voicemail	4-33
W	
warranty exclusions	Warranty-1
whitelist proxy	5-3
X	
XML SIP notify events	5-4



Disclaimer

Aastra Telecom Inc. will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use. While every effort has been made to ensure accuracy, Aastra Telecom Inc. will not be liable for technical or editorial errors or omissions contained within this documentation. The information contained in this documentation is subject to change without notice.

Copyright © 2012 Aastra Technologies Limited,
www.aastra.com.

