BluStar iOS Configuration Guide

FABRUARY 2015

RELEASE 3.2

Mitel®

Content

Administrator Configuration Guide and Configuration Key Reference for BluStar iOS Clients

Locked vs. Unlocked Version

The BluStar iOS Clients exist in a locked and unlocked version. The locked version can only be used on Aastra Call Managers. In order to use the BluStar client for non Aastra Call Managers / SIP Servers you need to purchase the full BluStar Version. Simply go to "Options" from the "Home" Screen and select "Purchase full version". Follow the instructions on the screen.

Please note that if you have trouble registering on Aastra Call Managers you should check for Video license availability there.

The below described configuration mechanisms apply to both Aastra and non-Aastra Call Managers / SIP servers.

BluStar iOS Configuration File Support

The BluStar iOS Clients can be configured manually, or via Aastra Configuration files similar to the Aastra SIP terminals. This document describes the configuration file support integrated into the BluStar iOS Version 1.2 and higher BluStar Clients. All documented configuration applies equally to the iPhone and iPad versions of the BluStar Client.

This document is intended solely to explain the configuration parameters available, and thus is intended primarily for Administrators familiar with the BluStar Clients (the “client”) wishing to automate the configuration or the rollout of the clients.

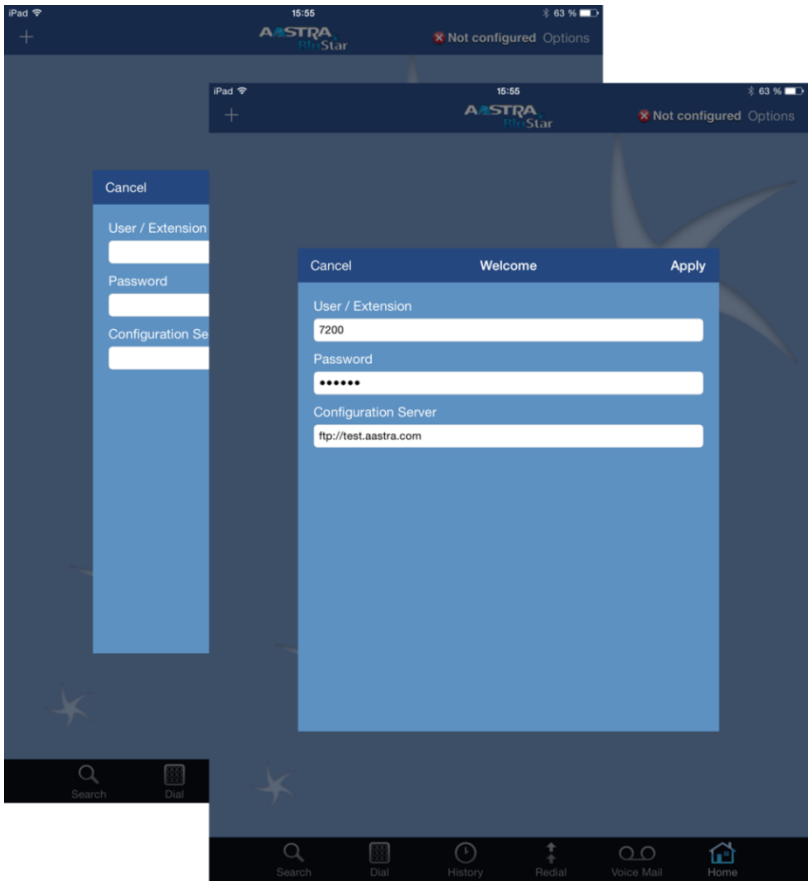
Configuration of the BluStar Client

The client supports delivery of configuration (.cfg) files via download from a configuration server as well as through email. There are three ways for the deployment:

- Provide an “aastra.cfg” configuration file via email to the iOS device with all information required
- Provide an “aastra.cfg” configuration file via email to the iOS device with basic information for the configuration server (IP address of FQDN) with or without “config user name” and “config user password”. The BluStar client it will download the configuration files from the configuration server (see below for details)
- Starting the BluStar client without having an “aastra.cfg” file on the device will make the BluStar client to prompt the user for the address of the configuration server, the “config user name” and “config user password” download the configuration files from the configuration server (see below for details).

Configuration Pop-up

When the client is opened for the first time and no configuration is present, a pop-up will prompt the user to enter the server name or IP address of the configuration server, along with the applicable username and password. If the entered information is correct, a valid configuration will be downloaded. See chapter 0 for



details about the files downloaded.

Note that the configuration file download can also be initiated by sending an incomplete configuration file via email as explained in chapter 0.

Delivery via Email

To use the email approach, the client must first be installed on the device. After the installation, an email with a configuration file as attachment can be sent to the device. The attachment must be named "aastra.cfg". It can contain arbitrary configuration keys as explained below.

To activate the configuration, the user must open the received email. The attachment will be displayed with the BluStar logo. If the attachment is not displayed with the BluStar logo, please make sure the file is named correctly and that the BluStar client installed. To activate the configuration click on the attachment and select that you want to open the file with BluStar. The client will come to the foreground and immediately apply the contained settings. All settings will become active on the fly. This means that if e.g. a SIP account is contained, the client should instantly start to register.

Please note:

- The email attachment must be called "aastra.cfg", otherwise it will not be picked up by the client (to avoid conflicts with other SW utilizing this extensions and protecting users from accidentally destroying their configuration opening such attachments)
- The "aastra.cfg" file contained in an email can be used to deliver a complete configuration, or just a "bootstrap" configuration pointing to a configuration server.
  Note: If a configuration server is contained in the "aastra.cfg" the client will first apply the settings contained in the email attachment then download the files from the configuration server (any other parameters like SIP related configuration information etc. will be ignored).
  The downloaded settings will also be activated on the fly.
- If essential configuration-server information is missing in the attachment, a pop-up for completion of said information will open.

Mixed Configuration via Email and File Download

This is a variation of the "delivery via email" approach allowing the administrator to take the burden from the user to type in the configuration server's address (and / or the configuration user name / password). Sending an "aastra.cfg" to the Android device attached to an email and opening it as described above will make the BluStar client to scan the file. If the information to register via SIP to a call server is not provided the BluStar client will try to download the configuration files from a configuration server. If "config user name / password" are not provided in the "aastra.cfg" the BluStar client will prompt the user for such data.

Note: This equals the behavior explained in chapter 0 (when the “aastra.cfg” contains config server parameters),

Configuration via File Download / Configuration Server

A configuration file can also be downloaded from a configuration server. To trigger the client to do this, you must use an email containing the configuration server parameters (as described above). The configuration server settings are not user accessible.

The client supports HTTP, HTTPS, FTP, and TFTP for downloading a configuration file from a server.

The client will fetch the files in the following order.

1. aastra.cfg
2. blustarios.cfg - This is the model specific configuration
3. <user >.cfg - where <user> is the name the user enters into the configuration pop-up which appears if no user name is specified in configuration file.

Configuration keys

SIP Accounts

The following settings configure the first and by default activated SIP account. Additional accounts can by configured by using the line[0-9] identifier.

Parameters in Configuration File	Description
sip [line0-9] user name:	User name used in the name field of the SIP URI for the BluStar and for registering the BluStar at the registrar. Valid values are all visible string characters. The field does not default to anything. For example:

	sip user name: lorem sip line1 user name: ipsum
sip [line0-9] password:	Password used to register the BluStar client with the SIP proxy. Valid values are all visible string characters. The field does not default to anything.
sip [line0-9] auth name:	The sip auth name is used on the authorization (REGISTER) on the PBX. If this setting is not set, the sip user name will be used. Default is empty and hence unconfigured. For example, sip auth name: 1234
sip [line0-9] proxy ip:	The IP address of the SIP proxy server the BluStar 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. Any valid hostname or IP address. For example, sip proxy ip: 192.168.0.101
sip [line0-9] proxy port:	The proxy server's port number. Default is 5060 if configuration key not present or empty. Must be a valid number in the range between 0- 65536 For example, sip proxy port: 5060
sip [line0-9] outbound proxy:	This is the address of the outbound proxy server. All SIP messages originating from the BluStar are sent to this server. For example, if you have a Session Border Controller in your network, you would normally set its address here. Default is empty and hence unconfigured. Must be a valid host name / IP address For example, sip outbound proxy: 10.42.23.13
sip outbound proxy port:	Sets the port that should be used for SIP messages that are sent to the sip outbound proxy (see above).
sip [line0-9] vmail:	Specifies the phone number / SIP URI of the voicemail system connected to the SIP account. This parameter specifies the phone number you dial from your BluStar to retrieve your voicemail. Default is empty.

	For example, sip vmail: 5000
sip [line0-9] forward all state:	Specifies the state of call forwarding for all incoming calls. Values are 0 and 1, 0 disables and 1 enables call forwarding. For example, sip forward all state: 1
sip [line0-9] forward all number:	Specifies the number, to which all incoming calls should be forwarded if call forwarding for all incoming calls is enabled. For example, sip forward all number: 5000
sip [line0-9] forward busy state:	Specifies the state of call forwarding in case the client is currently in a call (SIP or GSM). Values are 0 and 1, 0 disables and 1 enables call forwarding. For example, sip forward busy state: 1
sip [line0-9] forward busy number:	Specifies the number, to which incoming calls should be forwarded if the client is currently busy (in a call) and if call forwarding on busy is enabled For example, sip forward busy number: 5000
sip [line0-9] forward no answer state:	Specifies the state of call forwarding in case the client/user does not answer the call after a certain amount of time. For example, sip forward no answer state: 1
sip [line0-9] forward no answer number:	Specifies the number, to which incoming calls should be forwarded if the client/user does not answer the call and call forwarding on no answer is enabled For example, sip forward no answer number: 5000
sip [line0-9] presence server:	Specifies the presence server address For example, sip presence server: 192.168.1.1
sip [line0-9] presence port:	Specifies the port on which the presence server can be reached For example, sip presence port: 1234
sip [line0-9] presence user name:	Specifies the user name that is used to register with the presence server For example, sip presence user name: xyz

sip [line0-9] presence server user name:	Specifies the user name for presence server authentication. For example, sip presence server name: de.example.com\aUser
sip [line0-9] presence server user password:	Specifies the password for the presence server authentication. For example, sip presence server user password: aPassword
sip [line0-9] presence user password save:	Specifies, if the client should store the sip presence server user password permanently. 0: Don't store 1: Store. For example, sip presence user password safe: 1
sip [line0-9] presence outbound proxy:	Specifies the outbound proxy address to be used for presence. If not configured but sip outbound proxy is configured, the sip outbound proxy will be used. For example, sip presence outbound proxy: 192.168.1.5
sip [line0-9] presence outbound proxy port:	Specifies the outbound proxy port to be used for presence. If not configured but sip outbound proxy port is configured, the sip outbound proxy port will be used. For example, sip presence outbound proxy: 2345
sip [line0-9] screen name:	Specifies the name that will be shown on the local display (account list, status on home screen).
sip [line0-9] display name:	Specifies the name that will be used on initiating calls for displaying at the remote party.
sip [line0-9] uri dial direct:	Enables or disables direct uri dialing where an invite is sent directly to the specified domain instead of the registrar. Works only in combination with UDP as sip transport protocol. 0: Direct dialing disabled 1: Direct dialing enabled

	For example, sip uri dial direct: 1
sip [line0-9] uri dial direct exclusion list:	Specifies a comma separated list of domains for which direct uri dialing is not performed if enabled. Matching is done using backward search, so “aastra.com” would match “example1.aastra.com” and “example2.aastra.com” For example, sip uri dial direct exclusion list: domain.com, aastra.com, example.net
sip [line0-9] call mode	Specifies the desired default call mode, which allows enabling outgoing audio only calls. By default, the client performs audio + video calls. 0: Outgoing calls are audio only 1: Outgoing calls are audio + video call For example: sip call mode: 0

Miscellaneous SIP / Codec Parameters

Parameters in Configuration File	Description
sip transport protocol:	Defines the transport protocol used for all SIP accounts. Valid values are: 0 - User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) – also called TCP preferred in UI as it will use TCP when possible otherwise use UDP 1- UDP 2- TCP It is recommended to use tcp whenever possible as more effective battery management is in place with tcp connections. The default value is 1 meaning udp. For example, sip transport protocol: 2 Please note that for compatibility reasons with previous versions, the client will also accept udp, tcp as explicit parameter values.

sip dtmf method:	Sets the dual-tone multifrequency (DTMF) method used on the BluStar to send DTMF digits from the BluStar via INFO messages. You can set the DTMF method as RFC2833 or SIP INFO. Default is 0 (RFC2833). For example, sip dtmf method: 1
sip use basic codecs:	Determines whether HD codecs are to be offered or not. Default value is 0 meaning that G722 will be offered. When set to 1, the BluStar will only offer G711 as codecs.
sip customized codec:	The BluStar support ilbc as an additional codec. In order to enable ilbc as the primary codec offered, simply set the customized codec setting as follows: sip customized codec: payload=iLBC;ptime=30;silsupp=off,payload=0;ptime=20; silsupp=off, payload=8;ptime=20;silsupp=off The client also supports G729 as codec. To enable G729 as primary codec, simply set the customized codec setting as follows: sip customized codec: g729
config user name:	The username, which is used for initial config, download if provided in the .cfg file that is received via mail. For example, config user name: UserA
max h264 tx rate:	Specifies the maximum video data transmit rate allowed when in a call. Default value is 768. Valid values are: ‘1536‘, ‘1024‘, ‘768’, ‘512’, ‘384’, 192, ‘128’ (non matching value will be set to nearest supported one e.g. 850 to 768 accordingly). In versions < 1.3, the key has to be written with h.264 instead of h264. Version 1.3 supports both variants for compability. For example, max h264 tx rate: 768

max h264 rx rate:	Sets the maximum video receive rate that the client will indicate in AS line. All types of BluStar will honor this request. Default value is 768. Valid values are - ‘1536‘, ‘1024‘, ‘768’, ‘512’, ‘384’, 192, ‘128’ (non matching value will be set to nearest supported one e.g. 850 to 768 accordingly). In versions < 1.3, the key has to be written with h.264 instead of h264. Version 1.3 supports both variants for compability. For example: max h264 rx rate: 768
video max kbitrate:	Sets the maximum video send / receive rate that client will use. Please note that if present it will set both the aforementioned TX and RX settings. Default value is 768. Valid values are - ‘1536‘, ‘1024‘, ‘768’, ‘512’, ‘384’, 192, ‘128’ (non matching value will be set to nearest supported one e.g. 850 to 768 accordingly) For example, video max kbitrate: 768
call forward disabled:	Disables call forwarding for all user accounts and hides the call forwarding options menu entry. Values are ‘1’ for disabling call forwarding and 0 for enabling call forwarding.
visual enhancement:	Enables the visual enhanced icons/colorblind support. Applies to the icons used for presence. The setting is a global setting that is used for all configured lines/accounts. Values are ‘1’ for enabling and ‘0’ for disabling visual enhancement. For example, visual enhancement: 1
tos sip:	Specifies Types of Service (ToS) for SIP traffic. Valid values can be created in compliance with RFC 2474.
tos rtp:	Specifies Types of Service (ToS) for RTP traffic. Valid values can be created in compliance with RFC 2474.

tos rtp video:	Specifies Types of Service (ToS) for RTP Video traffic. Valid values can be created in compliance with RFC 2474.
log module sip:	Turns logging off or activates “basic” or “full” logging. Valid values are 0, 1, and 2, respectively.
upload system info email:	Email address to which traces and logs (debugging) are sent. Has to be a valid email address, for example: traces@example.com

Contacts and LDAP Parameters

Parameters in Configuration File	Description
exchange contacts enabled:	Select between using Exchange synced contacts as directory source or an LDAP directory. Default value is 0 indicating that the client will use LDAP. Valid values are 0,1 (0 LDAP Directory. If 1 select exchange contacts) For example, exchange contacts enabled: 0
ldap server:	Specifies the LDAP server hostname or IP address. This parameter handles multiple values, in the format “username:password@ldapserver:port”, where: • 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)

ldap base dn:	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”. For example, ldap base dn: dc=aastra, dc=com
ldap type:	Configure generic or Microsoft Active directory LDAP. Default value is 0, generic directory. Valid range is 0, 1, 2 - 0 means generic directory, 1 means Active Directory, 2 means custom directory. If set as custom directory you must set the below explained attribute settings and search filter. For example, ldap type: 2
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. J or 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 middle name attribute list: name, mname
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: name, title

ldap name suffix attribute:	Specifies the LDAP name suffix (e.g. M.Sc.) 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 suffix attribute list: name, suffix
ldap job title attribute list:	Specifies the LDAP job title (e.g. CTO) 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: name, jtitle
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 business state attribute list:	Specifies the LDAP business state (e.g. BC) for the attribute list. If this parameter contains more than one value, only the first matching value will be selected in the record.
ldap business country attribute list:	Specifies the LDAP business country (e.g. CA) 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: organization, bcountry
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. 1-416-468-3277) 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 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. 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 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 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. 1-416-468-1212) 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: bphone2, ophone2
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 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 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 web address attribute list:	Specifies the LDAP web address 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: homepage
ldap pager attribute list:	Specifies the LDAP pager number 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 pager attribute list: pager
ldap search filter:	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... When using the fuzzy search, all attributes which should be searched have to be in the search string twice. Once, for exact match, with wildcards (cn=*%*). Once, for fuzzy search, with the fuzzy operator and without wildcards (cn~=%) For example, ldap search filter: (&(objectClass=person)(|(cn=*%*)(cn~=%)))

When using custom ldap attributes, postalAddress is not evaluated. If the postalAddress is formatted according to RFC, $ signs will be displayed as they serve as a separator which is not being processed.

The following is an example LDAP configuration using a custom LDAP server:

```
ldap first name attribute list: gecos
ldap last name attribute list: sn
ldap company attribute list: o
```

```
ldap home phone 1 attribute list: homePhone
ldap email 1 attribute list: mail
ldap business phone 1 attribute list: telephoneNumber
ldap business postal code attribute list: postalCode
ldap business city attribute list: postalAddress
```

Cellular Data Usage Parameters

Parameters in Configuration File	Description
cellular data usage:	Control usage of cellular data channel. Default Value is 0 and will make client register via WIFI only. Valid values are 0, 1 - 0 – disabled, 1 – enabled (allows the client to register over cellular data channel and make calls via this data connection. If disabled the client will only register when associated to a Wi-Fi network) For example, cellular data usage: 1

Configuration Server Parameters

The BluStar iOS Client supports downloading its configuration from a configuration server. HTTP, HTTPS, FTP and TFTP are supported as transmit protocols. However, the client only supports one type of configuration server at a time. It will use the first one defined in the configuration file. If multiple ones are defined all but the first one will be ignored.

Parameters in Configuration File	Description
ftp server:	The FTP server's IP address or network host name. This will become effective after this configuration file has been downloaded into the BluStar. The server can also include the full path. For example, ftp server: 192.168.0.131 For example: ftp server: 192.168.0.131/configs/ftp

	Optional: You can also assign a username and password for access to the FTP server. See the following parameters for setting username and password.
ftp path:	Specifies the path name to where the configuration files are located on the FTP server for downloading to the BluStar. For example, ftp path: configs/ftp If the BluStar'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.
ftp username:	The username to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded to the BluStar. For example, ftp username: aastraconfig
ftp password:	The password to enter for accessing the FTP server. This will become effective after this configuration file has been downloaded into the BluStar. For example, ftp password: 1234
tftp server:	The TFTP server's IP address. 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. The server can also include the full path. For example, tftp server: 192.168.0.130 For example, tftp server: 192.168.0.130/configs/tftp
tftp path:	Specifies the path name to where the configuration files are located on the TFTP server for downloading to the BluStar.

	For example, tftp path: configs/tftp **Note:** Enter the path name in the form folderX\folderX. For example, blustarios\configfiles.
http server:	The HTTP server's IP address. This will become effective after this configuration file has been downloaded into the BluStar. The server can also include the full path. For example, http server: 192.168.0.132 For example, http server: 192.168.0.132/blustar/1 **Optional:** You can also assign an HTTP relative path to the HTTP server. See the next parameter (http path).
http path:	Specifies the path name to where the configuration files are located on the HTTP server for downloading to the BluStar For example: http path: blustar/1 If the BluStar's configuration 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.
http port:	Specifies the HTTP port that the server uses to load the configuration to the BluStar over HTTP. The default port is 80. For example: http port: 1025
http digest username:	The username to enter for accessing the HTTP server. The BluStar supports digest authentication. This will become effective after this configuration file has been downloaded to the BluStar. For example, http username: aastraconfig
http digest password:	The password to enter for accessing the HTTP server. The BluStar supports digest authentication. This will

	become effective after this configuration file has been downloaded into the BluStar. For example, http password: 1234
https server:	The HTTPS server's IP address. This will become effective after this configuration file has been downloaded to the BluStar. The server can also include the full path. For example: https server: 192.168.0.143 For example: https server: 192.168.0.143/blustar/1 **Optional:** You can also assign an HTTPS relative path to the HTTPS server. See the next parameter (https path).
https path:	Specifies the path name to where the configuration files are located on the HTTPS server for downloading to the IP BluStar For example: http path: blustar/1 If the BluStar client's configuration 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.
https port:	Specifies the HTTPS port that the server uses to load the configuration to the BluStar over HTTPS. The default port is 80. For example: https port: 1025
https digest username:	The username to enter for accessing the HTTPS server. The BluStar supports digest authentication. This will become effective after this configuration file has been downloaded into the BluStar. For example, https username: aastraconfig
https digest password:	The password to enter for accessing the HTTPS server. The BluStar supports digest authentication. This will become effective after this configuration file has been downloaded into the BluStar.

For example, https password: 1234

Client Utilized Port Ranges

The BluStar iOS client uses the ports as indicated below. Note that the client initiates most connections as outbound connections. The only listening connections are SIP in UDP mode (client listening on ports 5060 – 5069) as well as the RTP media ports.

Port Range	Description
21	FTP config download (if configured)
69	TFTP config download (if configured)
80	HTTP config download (if configured)
389	LDAP connections
443	HTTPS config download (if configured)
5060 – 5069	TCP/UDP depending on configuration for SIP signaling.
49152 - 65535	RTP for Audio and Video data