Installation and Configuration Guide

Aastra BluStar for PC 2.0

Aastra BluStar for PC delivers high-quality audio, HD video and access to a set of UCC features from a single client on the desktop directly integrated with Aastra's communication servers.

Aastra Telecom Sweden AB
Box 42214, SE-126 17 Stockholm, Sweden
Tel +46 8 568 67000
www.aastra.com

Date: 2012-05-16
Document No: ASE/APP/SW/0093/EN

Contents

1 Introduction

This document describes the basic steps for installing BluStar for PC and configuring the client using the configuration template (BSCpc.cfg).

2 System Requirements

For the latest information regarding requirements and compatibility information, please refer to release notes and Aastra InfoChannel: https://infochannel.aastra.com/ .

2.1 Supported Aastra Communication servers

- MX-ONE 5.0
- MX-ONE 4.1 SP4 (Softphone capability)

The available functionality will be determined by the capabilities and licenses in the MX-ONE version it is connected to.

- A5000 R 5.4 or later version
- A400 R 2.1 or later version

The difference between the audio and video capabilities is based on the IP licences of the communication server

2.2 Client Requirements

Recommended hardware for Softphone capabilities:

- CPU: Intel Pentium 4 1.4GHz or equivalent
- RAM: 512 MB
- Hard Disk: BluStar for PC requires 50MB disk space + .NET Framework 4 (Additional disc space required for log files)

Recommended hardware for Video capabilities:

- CPU: Intel Core 2 Duo 2.1 GHz or equivalent
- RAM: 2 GB
- Hard Disk: Hard Disk: BluStar requires 50MB disk space + .NET Framework 4 (Additional disc space required for log files)
- Accelerated DirectX9 graphics

Recommended hardware for HD Video capabilities:

- CPU: Intel Core i5 2,5 GHz equivalent
- RAM: 2 GB
- Hard Disk: Hard Disk: BluStar for PC requires 50MB disk space + .NET Framework 4 (Additional disc space required for log files)
- Accelerated DirectX9 graphics

Software:

- Windows 7, 32 & 64 bit
  - Enterprise Edition
  - Ultimate Edition
  - Professional Edition
- Windows XP SP3
- Microsoft Office 2003 Outlook 2003, 2007 and 2010

- If the user has no administrator privileges on the PC, .NET Framework 4 needs to be installed on the PC before BluStar for PC is installed.

2.3 Supported & tested headsets

BluStar for PC supports most USB headsets. During our tests following devices have been verified:

- Jabra Biz 2400 USB
- Jabra PRO 9470, 9465, 9450, 930
- Jabra GO 6470, 6430
- Jabra GN2000 USB
- Jabra UCVOICE series
- Logitech clearchat
- Plantronics Savi (400 & 700 Series) – UC wireless
- Sennheiser PC-36 USB headset

2.4 Supported Webcams

Web cameras requirements:

- Directshow compatible
- Minimum resolution: 160 x 120 at 15 to 30 fps
- Color format YUY2 or I420

BluStar for PC supports most USB web cameras. During our tests following devices have been verified:

- Creative webcam Live! socialize HD
- Creative webcam Live! InPerson HD
- Creative Optia AF webcam
- Logitech webcam B990 HD
- Logitech webcam PRO 9000 II
- Microsoft Lifecam studio

2.5 Supported systems for Integration

- Microsoft Lync 2010
- Microsoft Office Communicator 2007 R2
- IBM Lotus Sametime 8.0 or later

3 Installation

The installation package BluStarClientSetup.exe includes both a MSI package and a standard .exe setup.

3.1 Standard Installation

To install BluStar for PC as a standard installation, do the following:

1. Double-click **BluStarClientSetup.exe**

2. Select **Typical** or **Customized** installation

    a. Typical – Most common features

    b. Customized – Chose between the following features:
        i. Office Communicator 2007 integration
        ii. IBM Sametime Plug-In

3. When the Installation wizard completes, click **Finish**
   BluStar for PC is now ready to be used

Note: The user installing the client needs in this case have local administrator privileges.

3.2 Silent Installation Using MSI Package

BluStar for PC is also delivered as an msi package (BluStarClient.msi). This package can be deployed remotely using Group Policy, Microsoft SMS, Novell ZENworks, Altiris Notification Server, or a similar tool.

This is the recommended way to install if users do not have local administrator privileges.

Note: The following software products must be installed before the MSI package is deployed:

- Microsoft Visual C++ 2008 SP1 Runtime
- Microsoft Visual C++ 2010 Runtime
- Microsoft .NET Framework 4.0 Full

Make sure that the software installation or remote deployment of BluStar has correctly completed.

3.3 Silent Installation Using EXE Package

BluStar for PC can be installed using command line options:

```
BluStarClientSetup.exe /S /v"/qn"
```

`/S` instructs the installation loader (BluStarClientSetup.exe) to run silently.

`/v` passes parameters to the Windows Installer engine where **/qn** instructs the engine (msiexec) to run silently.

Additional parameters may be passed to Windows Installer engine to control selected features. Available features are:

Feature: `BluStar` - BluStar Application, Required.
Feature: `BluStarOC` - Office Communicator 2007 Plug-in
Feature: `Sametime` - Sametime Plug-in
Feature: `Localization` - Localization Files (Dutch, French, German, Italian, Spanish and Swedish)

An example command line to install the BluStar for PC application and the Office Communicator Plug-in would be:

```
BluStarClientSetup.exe /S /v"/qn ADDFEATURE=BluStar,BluStarOC"
```

Passing parameters to the Windows Installer engine should only be performed by users experienced with Windows Installer.

4 Configuration

The configuration of BluStar for PC is predefined in common configuration files in order to simplify the provisioning process. The definition of the configuration server where the configuration files are placed is done either in an .xml file or a .cfg file.

(In future versions of BluStar for PC only the .cfg file will be available in order to align with the terminal way of handling configuration.)

In version 2.0 of BluStar for PC one of the system configuration files, `BluStarConfig.xml` or `config.cfg`, is required to denote the address and login credentials for connection to the configuration server. It must be provided during deployment of the client.

The client downloads the client configuration files (see below), user-specific and user preferences settings from the configuration server that can be the communication server or another http server.

The configuration files are as follows:

- Client configuration: `BSCpc.cfg`
- User settings: `BSCpc_<user>.cfg`
- User preferences: `BSCpc_prefs_<user>.cfg`

The user needs to provide his BluStar for PC user name (= device number) and password (if required from the communication server) on initial client startup in order to retrieve configuration data from the configuration server.

4.1 Installation with existing .xml configuration

The `BluStarConfig.xml` can be configured for a group of users and the file can be included the installation roll out. `BluStarConfig.xml`, `BluStar.exe.config` and `BluStarPrefs.txt` will be converted to the new configuration file types (used to be aligned with terminal way of handling configuration):

- `BluStarConfig.xml` → `BSCpc.cfg` (system settings)
- `BluStar.exe.config` `BSCpc_<user>.cfg` (user-specific settings)
- `BluStarPrefs.txt` → `BSCpc_prefs_<user>.cfg` (user- and workplace-defined settings)

(The <user> is the user name (extension) of the current BluStar for PC user.)

The basic configuration server connection settings will be extracted from `BluStarConfig.xml` and `BluStar.exe.config` and will be saved in `Config.cfg`.

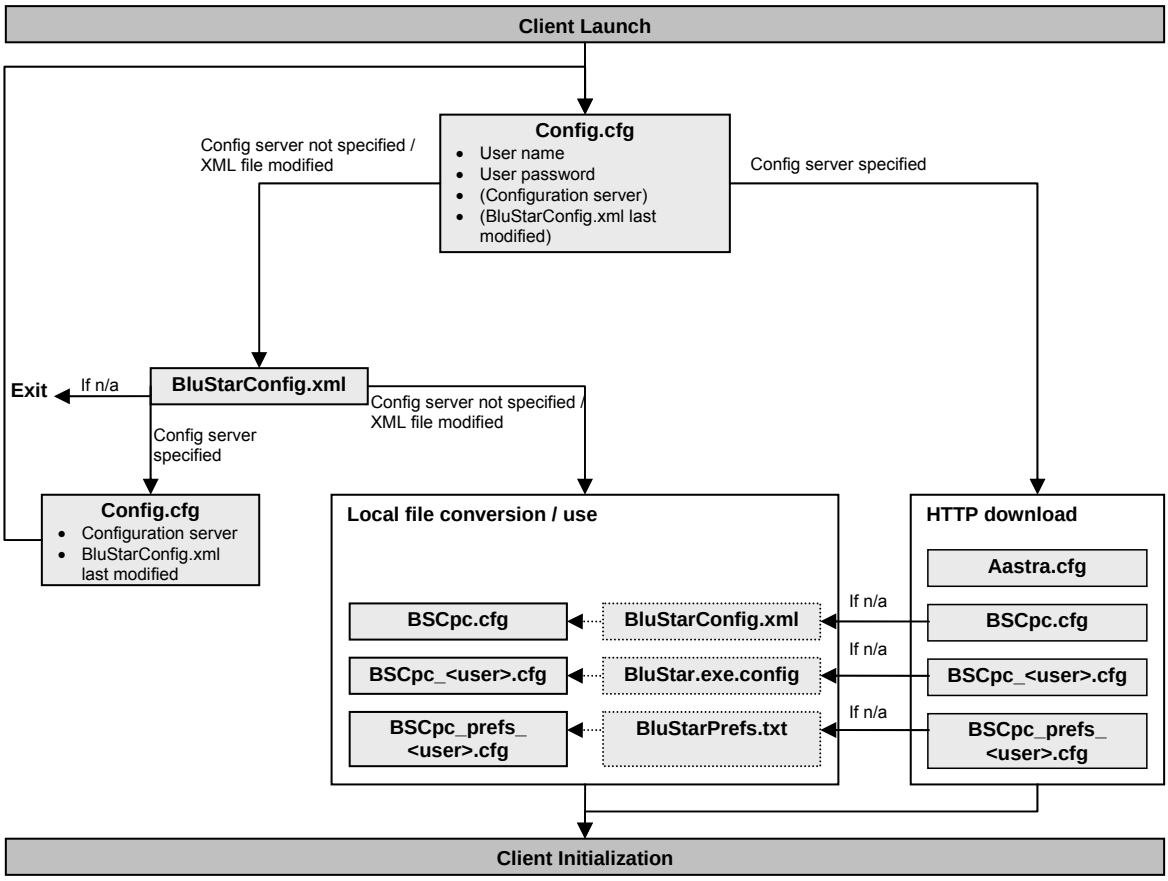
A few settings from the xml file characterized as user specific are exported to `BSCpc_<user>.cfg`.

The user will be prompted for user name and password when the client is started for the first time.

Future changes of the client options will only be stored in the .cfg files.

The .cfg files (except for `Config.cfg`) will be uploaded to the configuration server on client shutdown if a configuration server is defined in `BluStarConfig.xml` or in `Config.cfg`, otherwise the files are only stored locally.

Configuration workflow description:



4.2 Installation with configuration files (.cfg)

The `BSCpc.cfg` configuration file is used to configure system settings and defaults by a system administrator before installing BluStar for PC in the system environment.

When BluStar for PC is installed, the `BSCpc.cfg` file (together with the other configuration files) is downloaded to the client machine. On a US English machine the file is located:

Windows 7: `C:\Users\<User name>\AppData\Roaming\Aastra\BluStar\`
Windows XP: `C:\Documents and Settings\<User name>\Application Data\Aastra\BluStar\`

If a user client configuration file (`BSCpc_<user>.cfg`) already exists, the settings in this override the settings in the predefined client configuration when applicable.

Also the user settings override settings in the predefined client configuration when applicable.

Upload of changed user-defined settings to the configuration server takes place after each change.

Failover is supported when the configuration server is not reachable. BluStar for PC will use the local configuration files (if existing). Changed user settings will be stored locally.

`BSCpc.cfg` can be edited with any text editor.

4.2.1 Installation with configuration from configuration server

The user will be prompted for user name and password when the client is started for the first time.

If a configuration server address is provided in `config.cfg` or in `BluStarConfig.xml`, the client will connect to the specified server and retrieve the hosted client and user-defined configuration files. If no configuration server is defined or reachable, the client will use the system settings from `BluStarConfig.xml` according to section 4.2.1.

4.3 Capacity and Limitations

- The HTTP requests require a reply from the server within 10 seconds.
- The user needs read and write privileges for the following Windows system folder in order to temporarily store the configuration files:
  <APPLICATIONDATA>\Aastra\BluStar

5 Configuration parameters .xml file

See also document “Configuration Parameters – Aastra BluStar for PC 2.0"

Telephony Parameters	
SIPProxy	Enter the SIP proxy IP address or hostname and the proxy port number. *For example*: 10.20.30.40:5060 Default SIP port is 5060.
SIPOutboundProxy	Enter the Outbound SIP proxy IP address or hostname and the outbound proxy port number. *For example*: 10.20.30.40:5060 Default SIP port is 5060.
ConferenceAccessCode	Enter the access code for conference calls in the communication server. Please refer to communication server specific documentation if you do not know the code for conference. **Note:** If this field is left empty, the Conference button will be disabled. This field will be ignored if DisableConfTransferAccessCodes is set to true.
TransferAccessCode	Enter the code for transferring calls. Please refer to communication server specific documentation if you do not know the code for transfer. **Note**: For communication servers where Transfer code does not apply, leave this field empty. In this case, the SIP method Refer will be used. This field will be ignored if DisableConfTransferAccessCodes is set to true.
VoiceMailNumber	Enter the number to the Voice Mail System.
ConfigurationServer	Fully qualified URL of the configuration server
DisableIM	Enter **true** to disable Instant Messaging.
DisableVideo	Enter **true** to disable video teleconferencing.
TransportType	The transport type to use between PABX and BluStar for PC. Valid values are TCP(0), UDP(1).
QOSEnabled	Enter **true** to enable Quality of Service
QOSClass	The Quality of Service priority class. Valid values are Routine(0), AF class 1(1), AF class 2(2), AF class 3(3), AF class 4(4), AF class 5(EF), NetworkControl(7)
QOSDropPrecedence	The Quality of Service drop precedence. Valid values are Low(2), medium(4), and high(6).
DTMFType	The type of DTMF (End to end) tone to be used. Valid values are Info (0) and RFC2833 (2)
ActivateDTMFDigit	If the communication server requires a digit to be pressed to activate DTMF tones, enter this digit here.
DisableConfTransferAccessCodes	Set to **true** to disable the possibility to enter access codes in the UI.
Number Translation Parameters	
Enabled	Set to **true** to let BluStar for PC handle number translations. If set to true, specify the following number

	translation parameters. Set to **false** to let the communication server handle all number translations.
CountryCodeReplacement	Defines the string to replace the country code with when dialing
HomeAreaCode	Defines the area code that is to be ignored if it is included as a part of the dialed number.
HomeCountryCode	Defines the country code that is to be ignored if it is included as part of the dialed number.
InternationalAccessCode	Defines the access code to be used when a plus sign ("+") is encountered in the digit string. The plus sign ("+") will be replaced with the indicated digits.
LongDistanceAccessCode	Defines the access code for long distance calls. This access code will be dialed when a long distance number is detected for dialing.
MinimumDigits	Defines the maximum number of digits for a number dialed to be considered as an internal number. Any number dialed with more than the indicated number of digits will first cause the trunk access code to be dialed, then the digit string.
NumberFormat	Defines the dialing plan to be detected when performing number translation. Valid values are Standard (0), TAPI (1), and North American (2)
TrunkAccessCode	Defines the trunk access code digit(s) to be dialed prior to any external numbers.
ExceptionPrefixes	Defines the prefixes for which the trunk access code should not be dialed, regardless of the length of the digits entered by the user. For example, if a number with "850" in the beginning is dialed (8501234), the trunk access code will not be dialed prior to the digits entered, since "850" is in the exception list. This can be used to prevent the trunk access code from being dialed for private network calls.
InternalPrefix	Defines the prefixes that can be added to an internal extension number to define an external phone number.
Audio Codecs Parameters	
Codec	Set the order of audio codec to be used from BluStar for PC. Valid values are G722, SPEEX16, SPEEX8, ILBC, PCMU, PCMA and G729AB. The codecs PCMU, PCMA are G711.
Visible	Enter **true** to enable codecs.
LDAP Parameters (up to 5 LDAP directories can be configured)	
DisplayName	The display name shown in BluStar for PC.
HostName	The machine name where the LDAP directory resides.
Base	The organizational name that will be the starting point at which the LDAP server will start searching. Must be in LDAP format.

Port	The TCP/IP port number used to connect to the LDAP directory. Default is 389.
UserID	Optional. Only required for login if the LDAP directory is an Active Directory. You must use the SecEncrypter.exe tool to encode the UserID (more information can be found below).
Password	Optional. Only required for login if the LDAP directory is an Active Directory. You must use the SecEncrypter.exe tool to encode the UserID (more information can be found below).
DepartmentSearchField	The field to be used for the department search. This can be department, departmentName, organizationalUnitName or organizationName.
ActiveDirectory	Enter **true** if the LDAP directory is Active Directory, **false** otherwise.
IDField	Specifies the name of the LDAP field that uniquely identifies the record. Default = objectGUID if ActiveDirectory is true, distinguishedName if ActiveDirectory is false.
LastModifiedField	Specifies the name of the LDAP field that holds the last modified date/time. Default = whenChanged.
MaxTimeVariance	Specifies the maximum variance time in minutes between local time and the server time when determining if the record should be updated in the local cache. Default = 15.
PictureURL	Fully qualified URL of the location where pictures associated with directory records are stored, i. e. the storage location of user photos.
PictureExtension	File extension of the images (jpg, png etc.)
A5000 Parameters	(up to 5 A5000 directories can be configured)
DisplayName	The display name shown in BluStar for PC.
HostName	The machine name or IP address of the A5000.
Port	The TCP/IP port number used to connect to the LDAP directory. The default is 389.
UserID	You must use the SeCEncrypter.exe tool to encode the UserID (more information can be found below).
Password	You must use the SeCEncrypter.exe tool to encode the UserID (more information can be found below).
MultiSite	If the multi site feature is enabled in the A5000.
MultiSiteName	The name of the multi site installation (used instead of ou=local in the LDAP query)
IDField	Specifies the name of the LDAP field that uniquely identifies the record. Default = distinguishedName.
LastModifiedField	Specifies the name of the LDAP field that holds the last modified date/time. Default = whenChanged.
MaxTimeVariance	Specifies the maximum variance time in minutes between local time and the server time when determining if the

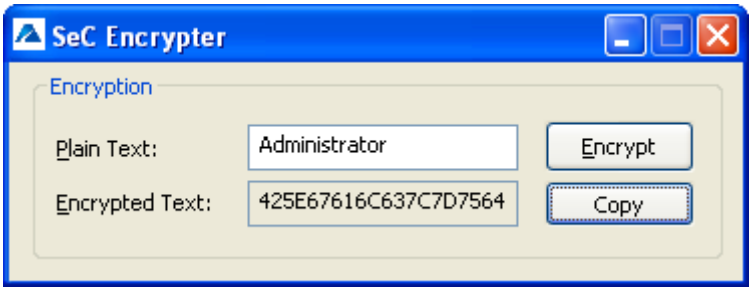
	record should be updated in the local cache. Default = 15.
PictureURL	Fully qualified URL of the location where pictures associated with directory records are stored, i. e. the storage location of user photos.
PictureExtension	File extension of the images (jpg, png etc.)
Error Reporting Parameters	
SentToMailAdress	Set prefix for mail adresses, if needed.
SendMethod	Valid values are SMTP, MAPI or empty.
Hostname	The host name of SMTP Server.
Port	The port to use towards SMTP Server.
SSL	Enter true to enable SSL protocol.
Authentication	Enter true to enable Authentication.
UserID	Optional. Only required for login if SMTPServer requires authentication. You must use the SecEncrypter.exe tool to encode the UserID (more information can be found below).
Password	Optional. Only required for login if SMTPServer requires authentication. You must use the SecEncrypter.exe tool to encode the UserID (more information can be found below).

5.1 SeC Encrypter Tool

To avoid storing user ids and passwords in plain text e.g. login credentials to the AD, the utility SeCEncrypter.exe is included in the BluStar for PC installation directory as well as copied to the application installation folder during installation. If encryption is required for a field, it will be noted in the field description.
To use SeC Encrypter, do the following:

1. Run SeCEncrypter.exe
2. Enter the data to be encrypted and click Encrypt.
3. Press Copy to copy the encrypted text to the clipboard

Paste it into the appropriate field in the XML configuration file.



5.2 Example File - BluStarConfig.xml

```
<?xml version="1.0" encoding="utf-8"?>
<BluStarClient>
 <Telephony>
       <User>
             <!-- format for SIPServer and SIPOutbound:  ipaddress of
server:portnumber.  e.g. 10.20.30.40:5060 -->
```

```
                  <SIPServer></SIPServer>
                  <SIPOutboundProxy></SIPOutboundProxy>
                  <ConferenceAccessCode></ConferenceAccessCode>
                  <TransferAccessCode></TransferAccessCode>
                  <VoiceMailNumber></VoiceMailNumber>
                  <MailAddress></MailAddress>

 <StoreCalendarDefinitionInAUCS>true</StoreCalendarDefinitionInAUCS>
                  <BluStarWebService></BluStarWebService>
            </User>
            <System>
                  <DisableIM>false</DisableIM>
                  <DisableVideo>false</DisableVideo>
                  <!-- XAastraIdModel values: 02=Voice, 03=CTI only,
04=Video  -->
                  <!-- XAastraIdOptions values: 01=Lync, 02=Sametime  -->
                  <XAastraIdModel>04</XAastraIdModel>
                  <XAastraIdOptions></XAastraIdOptions>
                  <!-- TransportType values: 0=TCP, 1=UDP  -->
                  <TransportType>1</TransportType>
                  <QOSEnabled>false</QOSEnabled>
                  <!-- QOSClass values:
                        0="000 Routine", 1="001 AF class 1", 2="010 AF
class 2", 3="011 AF class 3",
                      4="100 AF class 4", 5="101 AF class 5(EF)", 7="111
Network control"  -->
                  <QOSClass>0</QOSClass>
                  <!-- QOSDropPrecedence values: 2="010 Low", 4 ="100 Mid",
6 ="110 High" -->
                  <QOSDropPrecedence>2</QOSDropPrecedence>
                  <!-- DTMFType values: 0=Info, 2=RFC2833 -->
                  <DTMFType>0</DTMFType>
                  <ActivateDtmfDigit></ActivateDtmfDigit>

 <DisableConfTransferAccessCodes>false</DisableConfTransferAccessCodes>
                  <NumberTranslation>
                        <Enabled>false</Enabled>
                        <CountryCodeReplacement></CountryCodeReplacement>
                        <HomeAreaCode></HomeAreaCode>
                        <HomeCountryCode></HomeCountryCode>

 <InternationallAccessCode></InternationallAccessCode>
                        <LongDistanceAccessCode></LongDistanceAccessCode>
                        <MinimumDigits></MinimumDigits>
                        <!-- NumberFormat values: 0=Standard, 1=TAPI,
2=NorthAmerican -->
                        <NumberFormat>0</NumberFormat>
                        <TrunkAccessCode></TrunkAccessCode>
                        <ExceptionPrefixes>
                              <ExceptionPrefix></ExceptionPrefix>
                              <ExceptionPrefix></ExceptionPrefix>
                        </ExceptionPrefixes>
                        <ExtensionSize></ExtensionSize>
                        <InternalPrefixes>
                              <InternalPrefix></InternalPrefix>
                        </InternalPrefixes>
                  </NumberTranslation>
                  <!-- Note: The order the codes are listed here defines the
priority in which they will be used -->
                  <Codecs>
                        <Audio>
                              <Codec Visible="true">G722</Codec>
                              <Codec Visible="true">SPEEX16</Codec>
```

```
                              <Codec Visible="true">SPEEX8</Codec>
                              <Codec Visible="true">ILBC</Codec>
                              <Codec Visible="true">PCMU</Codec>
                              <Codec Visible="true">PCMA</Codec>
                              <Codec Visible="true">G729AB</Codec>
                        </Audio>
                  </Codecs>
            </System>
      </Telephony>
      <Directory>
            <LDAPDirectories>
                  <LDAP>
                        <DisplayName></DisplayName>
                        <HostName></HostName>
                        <Base></Base>
                        <Port>389</Port>
                        <!-- UserID and Password are optional but may be
required by your LDAP directory.
                              *** NOTE *** For security reasons, you must
run the SeCEncrypt utility,
                              copy and enter the encrypted data for these
fields-->
                        <UserID></UserID>
                        <Password></Password>
                        <!-- DepartmentSearchField values: 0=Department,
1=DepartmentName, 2=OrganizationalUnitName, 3=OrganizationName -->
                        <DepartmentSearchField>0</DepartmentSearchField>
                        <ActiveDirectory>false</ActiveDirectory>
             <!-- IDField: Specifies the LDAP attribute name of the field to
use to uniquely identify the directory items.
                Default = objectGUID for Active Directory, distinguishedName
for standard LDAP -->
             <IDField></IDField>
             <!-- LastModifiedField: Specifies the LDAP attribute name of
the field that hold the last modification time.
                Default = whenChanged -->
             <LastModifiedField></LastModifiedField>
             <!-- MaxTimeVariance: Specifies the maximum variance time in
minutes between local time and the server time when determining if the record
should be updated in the local cache.
                Default = 15 -->
             <MaxTimeVariance></MaxTimeVariance>
                        <Picture>
                              <PictureURL></PictureURL>
                              <PictureExtension></PictureExtension>
                        </Picture>
                  </LDAP>
            </LDAPDirectories>
            <A5000Directories>
                  <A5000>
                        <DisplayName></DisplayName>
                        <HostName></HostName>
                        <Port>389</Port>
                        <!-- *** NOTE *** For security reasons, you must run
the SeCEncrypt utility,
                              copy and enter the encrypted data for UserID
and Password -->
                        <UserID></UserID>
                        <Password></Password>
                        <MultiSite>false</MultiSite>
                        <MultiSiteName></MultiSiteName>
             <!-- IDField: Specifies the LDAP attribute name of the field to
use to uniquely identify the directory items.
```

```
                Default = distinguishedName -->
              <IDField></IDField>
              <!-- LastModifiedField: Specifies the LDAP attribute name of
the field that hold the last modification time.
                Default = whenChanged -->
              <LastModifiedField></LastModifiedField>
              <!-- MaxTimeVariance: Specifies the maximum variance time in
minutes between local time and the server time when determining if the record
should be updated in the local cache.
                Default = 15 -->
              <MaxTimeVariance></MaxTimeVariance>
                        <Picture>
                              <PictureURL></PictureURL>
                              <PictureExtension></PictureExtension>
                        </Picture>
            </A5000>
             </A5000Directories>
       </Directory>
       <ErrorReporting>
             <!-- When using MAPI, some clients require 'SMTP:' prefix for
mail addresses -->
             <SendToMailAddress></SendToMailAddress>
             <!-- SendMethod can be: SMTP, MAPI or left empty -->
             <SendMethod></SendMethod>
             <SMTPServer>
                   <HostName></HostName>
                   <Port></Port>
                   <SSL>false</SSL>
                   <Authentication>false</Authentication>
                   <UserID></UserID>
                   <Password></Password>
                   <!-- *** NOTE *** For security reasons, you must run the
SeCEncrypt utility,
                         copy and enter the encrypted data for UserID and
Password -->
             </SMTPServer>
       </ErrorReporting>
      </BluStarClient>
```

5.3 Model specific file (BSCpc.cfg)

For more information of configuration parameters .cfg files, see also document “Configuration Parameters – Aastra BluStar for PC 2.0"

5.3.1 Server and services connection settings

configuration server	Storage server for client/user configuration
sip proxy ip	Enter the SIP proxy IP address or hostname and the proxy port number. *For example*: 10.20.30.40:5060 Default SIP port is 5060.
sip proxy port	SIP proxy port
sip backup proxy	Backup SIP proxy IP address or hostname
sip backup proxy port	Backup SIP proxy port
sip outbound proxy	Enter the Outbound SIP proxy IP address or hostname and the outbound proxy port number. *For example*: 10.20.30.40:5060 Default SIP port is 5060.

sip outbound proxy port	Outbound SIP proxy port
sip backup outbound proxy	Backup outbound SIP proxy IP address or hostname
sip backup outbound proxy port	Backup outbound SIP proxy port

5.3.2 Client features

conf transfer access codes disable	Set to **true** to disable the possibility to enter access codes in the UI.
call conference feature code	Enter the access code for conference calls. Please refer to communication server specific documentation if you do not know the code for conference. **Note:** If this field is left empty, the Conference button will be disabled. This field will be ignored if DisableConfTransferAccessCodes is set to true.
call transfer feature code	Enter the code for transferring calls. Please refer to communication server specific documentation if you do not know the code for transfer. **Note**: For communication servers where Transfer code does not apply, leave this field empty. In this case, the SIP method Refer will be used. This field will be ignored if DisableConfTransferAccessCodes is set to true.
sip vmail	Number to the Voice Mail System.
aucs store calendar definition	
im disable	Enter **true** to disable Instant Messaging.
video disable	Enter **true** to disable video teleconferencing.
audioman tosbyte	Enter IP type of service for audio
videoman tosbyte	Enter IP type of service for video
sip transport protocol	The transport type to use between PABX and BluStar for PC. Valid values are TCP(0), UDP(1).
sip dtmf method	The type of DTMF (End to end) tone to be used. Valid values are Info (0) and RFC2833 (2)
sip dtmf feature code	If the communication server requires a digit to be pressed to activate DTMF tones, enter this digit here.
sip suppress codec list<n>	Shows corresponding **sip customized codec<n>** for selection in the client options if set to true
sip customized codec<n>	Set the order of audio codec to be used from BluStar for PC. Valid values are G722, SPEEX16, SPEEX8, ILBC, PCMU, PCMA and G729AB. The codecs PCMU, PCMA are G711.

5.3.3 Number translation

number translation	Set to **true** to let BluStar for PC handle number translations. If

enabled	set to true, specify the following number translation parameters. Set to **false** to let the communication server handle all number translations.
number translation new country code	Defines the string to replace the country code with when dialing
number translation home area code	Defines the area code that is to be ignored if it is included as a part of the dialed number.
number translation home country code	Defines the country code that is to be ignored if it is included as part of the dialed number.
number translation international feature code	Defines the access code to be used when a plus sign ("+") is encountered in the digit string. The plus sign ("+") will be replaced with the indicated digits.
number translation long distance feature code	Defines the access code for long distance calls. This access code will be dialed when a long distance number is detected for dialing.
number translation trunk feature code	Defines the trunk access code digit(s) to be dialed prior to any external numbers.
number translation minimum digits	Defines the maximum number of digits for a number dialed to be considered as an internal number. Any number dialed with more than the indicated number of digits will first cause the trunk access code to be dialed, then the digit string.
number translation number format	Defines the dialing plan to be detected when performing number translation. Valid values are Standard (0), TAPI (1), and North American (2)
number translation trunk exceptions	Defines the prefixes for which the trunk access code should not be dialed, regardless of the length of the digits entered by the user. For example, if a number with "850" in the beginning is dialed (8501234), the trunk access code will not be dialed prior to the digits entered, since "850" is in the exception list. This can be used to prevent the trunk access code from being dialed for private network calls.
number translation extension length	Enter the number of digits for internal extension. This parameter is also needed for showing picture from a database.
number translation internal prefix	List the number prefixes that could be added to internal extension to define external number.

5.3.4 LDAP directories

Configuration can contain multiple directories (up to 5). Directory parameters are numbered with the same index number <n> for each directory; the different directories are consecutively numbered starting with 1.

ldap<n> name	The display name shown in BluStar for PC
ldap<n> server	LDAP directory host. Combines user ID, password, host name and port in the expression '<user ID>:<password>@<host name>:<port>'. User ID and password need to be encrypted. The directory will be discarded if this parameter is empty.
Ldap<n> version	LDAP database version

ldap<n> base dn	The organizational name that will be the starting point at which the LDAP server will start searching. Must be in LDAP format.
ldap<n> field department search	The field to be used for the department search. This can be department, departmentName, organizationalUnitName or organizationName.
ldap<n> activedirectory	Enter **true** if the LDAP directory is Active Directory, **false** otherwise.
ldap<n> field id	Specifies the name of the LDAP field that uniquely identifies the record. Default = objectGUID if ActiveDirectory is true, distinguishedName if ActiveDirectory is false.
ldap<n> field last modified	Specifies the name of the LDAP field that holds the last modified date/time. Default = whenChanged.
ldap<n> max time variance	Specifies the maximum variance time in minutes between local time and the server time when determining if the record should be updated in the local cache. Default = 15.
ldap<n> server image uri	URL to access picture of users in CMG database linked to this LDAP directory
ldap<n> picture extension	extension of user picture files (could be jpeg, png, ...)

5.3.5 A5000 directories

a5000<n> name	The display name shown in BluStar for PC.
a5000<n> server	A5000 server. Combines user ID, password, host name and port in the expression '<user ID>:<password>@<host name>:<port>'. User ID and password need to be encrypted. The directory will be discarded if this parameter is empty.
a5000<n> multi site	If the multi site feature is enabled in the A5000.
a5000<n> multi site name	The name of the multi site installation (used instead of ou=local in the LDAP query)
a5000<n> activedirectory	Indicates whether directory is an AD directory
a5000<n> field id	Specifies the name of the LDAP field that uniquely identifies the record. Default = distinguishedName.
a5000<n> field last modified	Specifies the name of the LDAP field that holds the last modified date/time. Default = whenChanged.
a5000<n> max time variance	Specifies the maximum variance time in minutes between local time and the server time when determining if the record should be updated in the local cache. Default = 15.
a5000<n> server image uri	URL to access picture of users in the A5000 database
a5000<n> picture extension	extension of user picture files (could be jpeg, png, ...)

5.3.6 Error reporting

upload system info email adress	Set prefix for mail adresses, if needed.

upload system info email method	Valid values are SMTP, MAPI or empty.
upload system info smtp server	The ip address or host name of SMTP Server.
upload system info smtp server port	The port to use towards SMTP Server.
upload system info smtp encryption	Specifies if a SSL (encrypted) connection is to be used when connecting to the SMTP server
upload system info smtp auth enabled	Enter true to enable Authentication.
upload system info smtp auth name	Optional. Only required for login if SMTPServer requires authentication. You must use the SecEncrypter.exe tool to encode the UserID (more information can be found below).
upload system info smtp auth password	Optional. Only required for login if SMTPServer requires authentication. You must use the SecEncrypter.exe tool to encode the UserID (more information can be found below).

5.4 User specific file (BSCpc_<user>.cfg)

The user specific file is associated with the current client user via the BluStar for PC user name (i.e. extension number) <user> as part of the file name.

5.4.1 Server and services connection settings

telephony extension	Enter User's extension number (login ID)
telephony extension password	Enter User's login password
sip proxy ip	Enter SIP proxy IP address/host name
sip proxy port	Enter Enter SIP proxy port
sip outbound proxy	Enter outbound SIP proxy IP address/host name
sip outbound proxy port	Enter outbound SIP proxy port
sip reregistration time	SIP session duration (in seconds)

5.4.2 Licensing

x aastra id model	License type (model definition). Available values are: 02 (Softphone), 03 (CTI client), 04 (Video Softphone)
x aastra id options	License type (client feature definition). Available values are: 01 (Plug-in MS OCS/Lync), 02 (Plug-in IBM Sametime)

5.4.3 Client features

sip vmail	Enter the user's voice mail number

user mail address	Enter the user's mail address
network type	Enter used IP network type
video bitrate	Video stream bitrate
video quality	Video stream resolution and quality

5.4.4 Directory settings

directory outlook enabled	Enables use of Outlook directory
directory outlook profile	Outlook directory profile name
directory cache update interval	Interval for updating directory cache (in seconds)
directory cache delete interval	Interval for deleting the directory cache (in milliseconds)

5.4.5 Telephony features

telephony sound file busy	Sound file for busy signal
telephony sound file calling	Sound file for call signal
telephony sound file ringing	Sound file for ringing signal
call conference feature code	Access code for conferences
call transfer feature code	Access code for call transfers
telephony codecs	List of available telephony codecs
telephony automatic echo cancellation	Enables automatic echo cancellation for audio output devices
telephony automatic gain control	Enables automatic gain control for audio input devices

5.4.6 Logging

sip log level	SIP client log detail level
log level	Client log detail level
max log files	Maximum number of log files

6 Video Quality

Making video calls over a network with insufficient performance will cause degradation of the quality of the video call. Especially, this can be the case when using a wireless office network. If video quality issues occur when using wireless network, it is recommended to use a wired nework instead if such a network is available.

Also if a video issue occurs when CPU load is high, it is recommended to use video settings of less quality.

Sometimes an attempt to change to wired network can be unsuccessful due to existing network settings in Windows. To make the Local Area Connection (the term for wired local network in Windows) the default network, follow the procedures below.

To give Local Area Connection first priority, proceed as following:

1. In the **Control Panel**, open **Network Connections** (in Windows 7; Network Internet → Network Connections).
2. Select **Advanced → Advanced Settings…**
3. In the **Advances Settings** window, **Connections** area, the Local Area Connection should be at the top. If not, use the up and down keys to rearrange the list.
4. Click **OK**.

In Windows, the interface metrics can be set for the network adapters. If Automatic metric is enabled, the default setting is 10. Setting a higher metric for wireless than wired network should make the wired network the preferred network.

To change the metric for the wireless network, proceed as following:

1. In the **Control Panel**, select **Network Connections** (in Windows 7; Network Internet → Network Connections) and **Wireless Network Connection**.
2. Select **Wireless Network Connection Properties**. Click **Internet Protocol (TCP/IP)**, followed by **Properties**.
3. In the **Internet Protocol (TCP/IP) Properties** window, click **Advanced…**
4. Disable **Automatic metric**. In the **Interface metric** text field, set the value to **50**.
5. Click **OK**.

7 Integration

7.1 Integration with CMG LDAP

To take advantage of the CMG LDAP integration, CMG 7.5 SP2 needs to be installed on the CMG server, see the Installation and Configuration Guide of CMG 7.5 SP2.

To configure BluStar for PC towards CMG LDAP directory, see the parameters in sections: “Configuration parameters .xml file" and “Configuration parameters .cfg file".

7.2 Integration with Image Sources

BluStar for PC can be integrated with the image source in Aastra’s products CMG Application Suite and Aastra 5000. Pictures that already exist in the database for either of these products can then be displayed directly in the contact list and contact cards of BluStar for PC.

7.2.1 Integration with Image Configuration .xml file

In the `BluStarConfig.xml` file the following parameters (marked in bold) need to be configured to retrieve pictures from the databases:

```
<?xml version="1.0" encoding="utf-8"?>
<BluStarClient>
[.....]
 <Telephony>
  <NumberTranslation>
   [.....]
   <ExtensionSize>5</ExtensionSize>
   <InternalPrefixes>
    <InternalPrefix>+468xxx</InternalPrefix>
    <InternalPrefix>00468xxx</InternalPrefix>
    <InternalPrefix>08xxx</InternalPrefix>
   </InternalPrefixes>
  </NumberTranslation>
 </System>
</Telephony>
<Directory>
 <LDAPDirectories>
  <LDAP>
   <DisplayName>Name of directory</DisplayName>
   <HostName>IP / hostname of directory server</HostName>
   <Base>dc=aastra,dc=com</Base>
   <Port>3268</Port>
   <!-- UserID and Password are optional but may be required by your LDAP directory.
     *** NOTE *** For security reasons, you must run the SeCEncrypt utility,
    copy and enter the encrypted data for these fields-->
   <UserID></UserID>
   <Password></Password>
   <!-- DepartmentSearchField:  0=Department, 1=DepartmentName,
2=OrganizationalUnitName,3=OrganizationName -->
   <DepartmentSearchField>0</DepartmentSearchField>
   <ActiveDirectory>true</ActiveDirectory>
   <Picture>
       <PictureURL>http://10.105.21.60/CMGOffice/subscriberimages/</PictureURL>
       <PictureExtension>jpg</PictureExtension>
   </Picture>
  </LDAP>
 </LDAPDirectories>
 <A5000Directories>
```

```
<A5000>
 <DisplayName>Name of A5000 directory</DisplayName>
 <HostName>IP / hostname of A5000 directory</HostName>
 <Port>389</Port>
 <UserID>xxx</UserID>
 <Password>xxx</Password>
 <MultiSite>false</MultiSite>
 <MultiSiteName></MultiSiteName>
 <Picture>
     <PictureURL>http url to picture database</PictureURL>
     <PictureExtension>png/jpg</PictureExtension>
 </Picture>
</A5000>
</A5000Directories>
</Directory>
</BluStarClient>
```

7.2.2 Integration Image Source Configuration .cfg file

In `BSCpc.cfg` specific file following parameters needs to be configured to retrieve pictures from the databases:

number translation extension length	Enter the number of digits for internal extension. This parameter is also needed for showing picture from a database.
ldap<n> server image uri	URL to access picture of users in CMG database linked to this LDAP directory
ldap<n> picture extension	extension of user picture files (could be jpeg, png, ...)
a5000<n> server image uri	URL to access picture of users in the A5000 database
a5000<n> picture extension	extension of user picture files in the A5000 database (could be jpeg, png, ...)

7.3 BluStar for PC Plug-In integration for Microsoft OCS / Lync

The Microsoft OCS / Lync Plug-In feature for Aastra BluStar for PC will be pre-selected during installation if Office Communicator or Lync is installed on the PC.

If Office Communicator or Lync is installed after BluStar for PC is installed, the BluStar for PC installation must be re-run with the BluStar for PC OCS / Lync Plug-In feature selected. The users need to log in to BluStar for PC with a SIP extension in order to use call handling.

The plug-in provides basic call handling using BluStar for PC behind Office Communicator. To call a contact in Office Communicator using BluStar for PC, drag and drop the contact to the BluStar for PC call window.

The Microsoft Lync 2010 integration will enable the user to initiate BluStar for PC audio, video or IM session from within the Lync application by right clicking on a contact in the contact list and selecting the menu choice to start a Blustar for PC audio, video or IM session.

To be able to use the BluStar for PC MS OCS / Lync integration a *BluStar for PC Lync/OCS Plugin* license is needed for the user (extension).

Note, there is no presence integration between Office Communicator / Lync and the BluStar for PC plug-in in version 2.0.

7.3.1 Launch BluStar for PC Automatically

Launching BluStar for PC when Office Communicator or Lync is started can be done in two ways:

- From BluStar for PC menu Options…, select Launch at Windows Logon.
- Edit the registry parameter LaunchBluStarClient

Registry parameter:

```
HKEY_CURRENT_USER\Software\Aastra\BluStarClientOC\LaunchBluStarC
lient
REG DWORD
```

1 = Launch BluStar
0 = Do not launch BluStar
Default is 0.

7.4 BluStar for PC Plug-In for Sametime

The Aastra BluStar for PC plug-in for Sametime can be installed and integrated in two different ways:

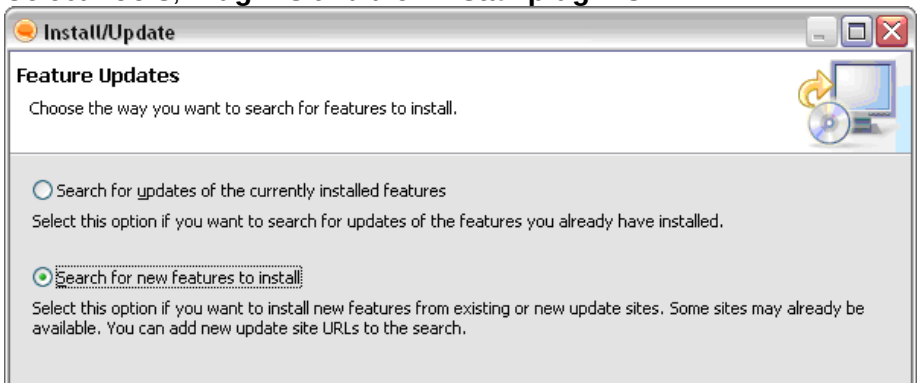
1. **Manual Installation** – Lotus Sametime Connect Users can install the plug-in manually using the Manage Updates user interface in Sametime Connect.
2. **Managed installation** – The Sametime administrator can automatically provision to all users in a specific community. The plug-in is automatically downloaded to the Sametime client when the user launches Sametime.

7.4.1 Manual Installation

To install BluStar for PC plug-in in Sametime Connect manually, the Sametime administrator has to enable this feature for users. This is done by checking the option Allow plug-ins installation in the Sametime Default Policy using Lotus Sametime Administration console. If the option is not enabled, the users are not able to install plug-ins manually and the only way to install them is using managed installation as described in 7.4.2 Managed Installation.

The following steps describe how to install the Aastra BluStar for PC plug-in files in Sametime Connect:

1. Select **Tools**, **Plug-ins** and then **Install plug-ins**



2. Select the option **Search** for new features to install and click Next in the Feature Updates window.

3. Select **Add Folder Location** and navigate to the Sametime folder where the Aastra BluStar for PC Sametime plug-in is located, for example C:\ Program Files\ Aastra\ BluStar Client\ Sametime. Select the folder and click OK. The new location is now visible in the list of Applications Locations. Click **Next**.

4. Select **Only show the latest version of a feature per update site** in the Search Results window. Expand the tree under BluStar Client/Sametime and select BluStar Integration Feature.

5. Click **Next**, read and accept the license agreement.

6. Click **Next** and review plug-in features to be installed.

7. Click **Finish** to install the plug-in files.
   After installation, Sametime Connect needs to be restarted for the changes to take effect.

7.4.2 Managed Installation

Managed Automatic Installation
In a Managed Automatic Installation, a Sametime update site URL needs to be specified on each of the Sametime servers. To construct this URL, first the content of BluStarClientSametimeInt.zip package has to be moved to a folder accessible via a web server. For example, if using a Lotus Domino Web Server, create subfolder BluStarClient under Lotus/Domino/Data/domino folder. Unpack the content of BluStarClientSametimeInt.zip into the created folder. In this case the update site URL will be: http://serverHostname/BluStarClient/site.xml.

Start the Sametime Administration Tool and select Policies, update the policies as follows:

1. Locate the **Sametime update Site URL** setting in the **Instant Messaging** section of the policy.

2. Enter the update site URL. If more than one URL needs to be specified they have to be separated by semi-colons or commas. Click **OK** to save the changes and close the policy editor.

When the users start Sametime Connect application, BluStar for PC Integration plug-in will be silently downloaded from the update site and installed automatically. Once installation is complete, the user receives a textbox announcing that a new plug-in has been installed and that the user should restart the Sametime client.

Managed Optional Installation
An alternative to the managed automatic installation is an optional installation. In this case, the new plug-ins and updates from the predefined update sites will not be installed for the Sametime client users automatically, but the users will be presented an option whether to install new plug-ins or not. A user of Sametime Connect can also manually check for optional updates by selecting **Tools**, **Plug-Ins** and **Check for Optional Plug-ins**.

To set up a managed optional installation on the server, prepare an update site and create the update site URL in the same as way as described in section 0
Managed Automatic Installation Start Sametime Administration Tool and select **Policies**. Each of the appropriate policies has to be updated in the following way:

1. Locate the **Sametime optional add-on site URL** setting in the **Instant Messaging** section of the policy.

2. Enter the update site URL. If more than one URL needs to be specified they have to be separated by semi-colons or commas. Click **OK** to save the changes and close the policy editor.

7.4.3 Removing BluStar for PC Integration Plug-In from Sametime

You can remove the BluStar for PC Integration plug-in using the standard Sametime feature removal tools. Complete the following steps:

From the Sametime Connect application, select **Tools, Plug-Ins** and **Manage Plug-ins**.

In the Application Management window, expand sections in the tree and find the feature **BluStar Integration Feature** x.x.x in the list. Right-click the feature name and then select **Uninstall**.

Aastra Technologies Limited
Concord, Ontario, Canada