BluStar Server 3.2
Installation and Configuration Guide

JAN 2015

REV A

ADMIN GUIDE

Mitel®

Contents

1 Introduction to BluStar Server

The BluStar Server is an element of the BluStar Ecosystem which provides “Presence” and “Directory Lookup” capabilities to the BluStar clients

- The term “Presence” describes the user’s availability composed from presence sources such as calendar entries, line state and manual status settings
- The term “Directory Lookup” describes the ability of the BluStar Server to connect to various directory sources for the purpose of load reduction / performance improvements and directory search result consolidation

The BluStar server is built by three main components:

- Presence Server as the connection to the presence sources / calendar systems
- CTI Server as connection to the communication server for retrieving line state information and providing CTI functionality
- Aastra Directory Server for directory queries of BluStar clients

For leveraging the BluStar Server BluStar clients are required

- Mitel 8000i with software V 4.3.0 or higher
- Mitel BluStar for PC V 3.0 or higher
- BluStar for iPhone and BluStar for iPad v3.0 or higher.
- MMC Controller 4.1 with MMC 4
- Mitel InAttend
- MiVoice Office 400

The BluStar clients can show presence information i.e. on their “Favorites” screens. For all users / extensions for which presence information is to be displayed the BluStar clients will subscribe on the BluStar Server which will fetch appropriate information from various sources. Thus the BluStar client may have one IP connection to the communication server and a separate connection to the BluStar Server, this must be considered for the networking as well as for the router and / or Session Border Controller configuration.

The BluStar Server can support multiple communication servers, presence sources and directories at the same time.

This document provides information about the installation and configuration of the BluStar Server.

1.1 Architecture

The main components of the BluStar Server are using TCP/IP connections for inter-component communication. It is not recommended to change the related settings.

The BluStar Server component “Presence Server” consolidates calendar information, line state and manual user status settings for every user.

The BluStar Server component “CTI Server” (including TR87) monitors the line state of all users / extensions for which a BluStar client has made a subscription.

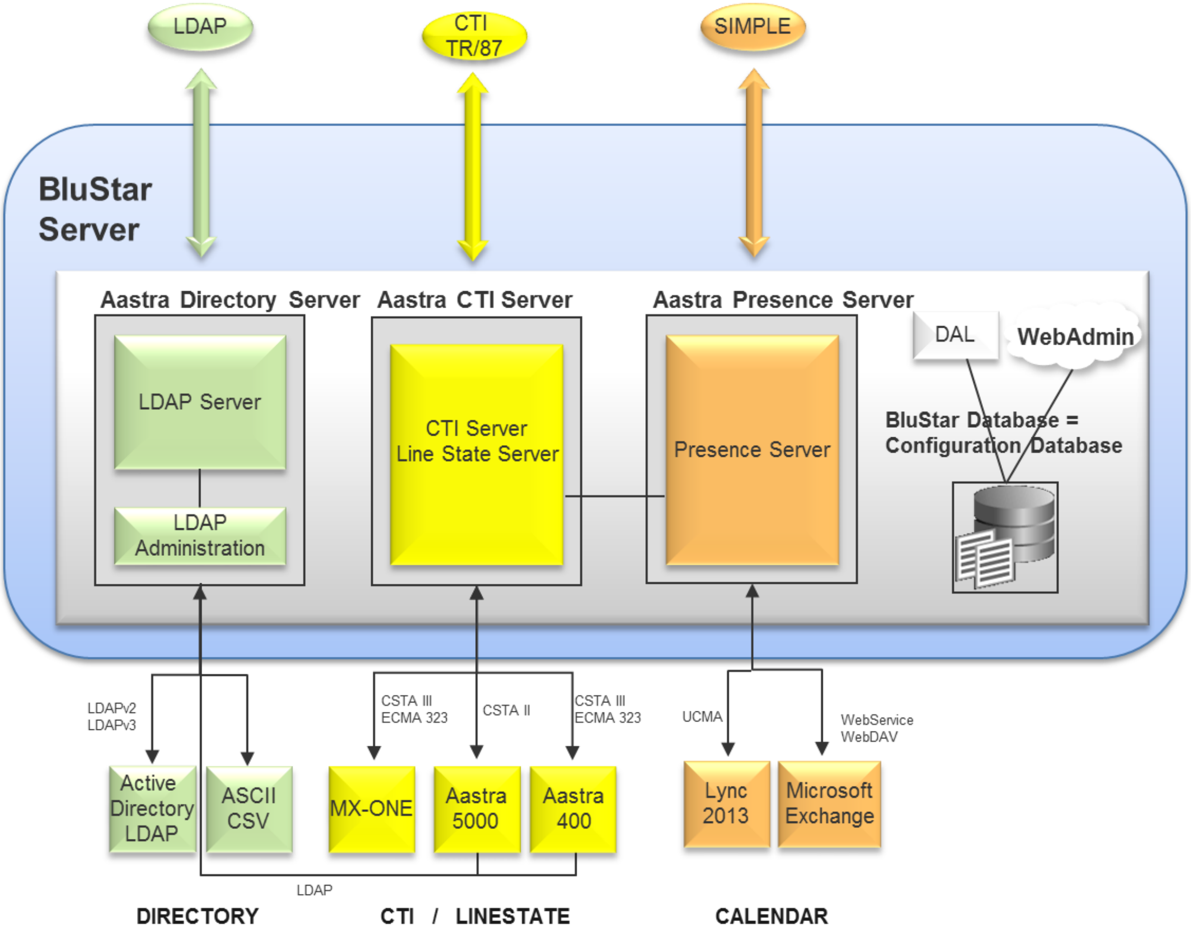
The BluStar Server component “Aastra Directory Server” is basically a caching proxy for directory lookups. Please note that the BluStar Server does not host its own directory database (aside from the ability to consider local ASCII-files for directory lookups), it always refers to “higher authority” databases such as the directory service of a communication server or Active Directory services and caches their content.

1.1.1 Scalability, multi-server installations

The BluStar Server performance has been validated under various user case scenarios for both “real hardware” and when used virtualized with VMware vSphere V 5.1.

1.1.2 Overview about the main components of the BluStar Server

The following picture provides an overview for the main components of the BluStar Server:



1.2 Notes on guarantee and warranty

- Aastra accepts no warranty claims for malfunctions and limited functionality caused by non Aastra-Applications installed by the customer.
- Please also note the guarantee and warranty conditions from Microsoft relating to the Windows operating system or other Microsoft components in use.
- Aastra accepts no warranty claims for malfunctions on 3rd-party components delivered together with BluStar Server.

For more details see the end user license agreement for BluStar.

2 Terminology

2.1 ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
CSTA	Computer-Supported Telecommunications Applications
CTI	Computer Telephony Integration
CSV	Comma Separated Values
DAL	Data Access Layer
LDAP	Lightweight Directory Access Protocol
OCS	Office Communications Server
PIDF	Presence Information Data Format
RPID	Rich Presence extensions to PIDF
SOAP	Simple Object Access Protocol
(SIP) SIMPLE	Sip for Instant Messaging and Presence Leveraging Extensions
WebDAV	Web Distributed Authoring and Versioning

3 BluStar Server installation

3.1 Planning and designing

The BluStar Server must be accessible for all BluStar clients based on their IP network connections such as LAN, WLAN, GSM / LTE. Appropriate security must be provided by the network design using Firewalls and / or Session Border Controllers when appropriate.
Please note that the IP-address of the BluStar Server may have to be resolved differently on the LAN or when accessed from the Internet.

3.2 TCP and UDP ports used

All TCP and UPD ports required to access the BluStar Server (direction: towards the BluStar Server) are listed below, to be considered for Firewall / Session Border Controller configuration.

Port	TCP	UDP	Protocol	Points to ...	Used for
80	✓	-	http	MS IIS web server	Web administration
8080	✓	-	http	Apache web server	Notification service for MS Exchange
389	✓	-	LDAP	BluStar Server Directory Server	BluStar clients for directory access
5060	✓	✓	SIP	BluStar Server Presence Server	BluStar clients for presence
5070	✓	-	SIP	BluStar Server CTI Server	BluStar clients for CTI via TR/87

Please note:

- the BluStar Server needs to connect to AD for LDAP access on port 3268 (outgoing from BluStar Server)
- when an external SQL server is used, the BluStar Server must be able to access it on port 1433 / TCP

3.3 Before the installation

Best is to assure that the destination server fulfills the appropriate hardware and software requirements. Hardware requirements can be found in the corresponding product specifications.
Please check the network routing to ensure that the BluStar Server can connect to all presence sources, communication servers and calendar servers on the appropriate transport protocols and ports.
A decision must be taken if the BluStar Server shall be used with Microsoft SQL Server 2012 Express or if a Microsoft SQL Server which already exists shall be used.

3.4 HW requirements of BluStar Server

- CPU: 2,2 GHz or faster,
- 2 cores recommended
- RAM: 8 GB
- Hard drive: 10 GB available space
- Network: GigE network adapter

For vSphere 5.1 based virtualized environments the HW requirements do not differ for the virtual machine; the actual performance will depend on the overall load of the machine hosting the VMs.

3.5 Operating system and software requirements for the BluStar Server

For the BluStar Server the Microsoft Server 2008 R2 SP1 and Microsoft Server 2012 SP1 are supported. Following the steps below will give you a clean installation of Microsoft Server 2008 ready to install BluStar Server. Maybe you have an installation you want to add BluStar Server to (including Windows Server 2012), then the list below can be used as a checklist for that installation.

- Run Windows setup, if possible with the ‘new installation’ option.
- Select ‘Windows 2008 R2 Standard (full install).
- After setup is completed, install virus protection software.
- If required, download and install SP1.

A window with initial server setup tasks is displayed. Work your way from top to bottom and follow the instructions below.

- Activate Windows.
- Set your time zone.
- Set the computer name (restart required).
- Enable automatic updates.
- Download and install updates (this may take several hours).
- Add server roles:
  - Server Role Application Server with enabled:
    - <Web Server (IIS) Support>
  - Server Role Web Server IIS with enabled:
    - <Static Content>
    - <Directory Browsing>
    - <HTTP Errors>
    - <ASP.NET>
- Add Features
  - .NET 3.5
- Optional: enable remote desktop

- Java Development Kit 1.7 or higher (64bit) must be installed
- Microsoft .NET framework.
  - 4.0 (download and install)
  - Windows Server backup
- Install SQL Server (express) if required.
  - Located in the BluStar Server installation package: x64\SQLEXPR_2012_x64.exe
  - Use Mixed mode as authentication method and set the ‘sa’ password according to the complexity requirements
  - Enable SQL browser feature

3.6 BluStar Server in a VMware vSphere environment

This section describes important information for running a BluStar Server in a VMware environment. As in the previous section, many different environments are possible, it is your own responsibility to set your operating system correctly. We cannot give support on this.

3.6.1 System requirements for VMware vSphere

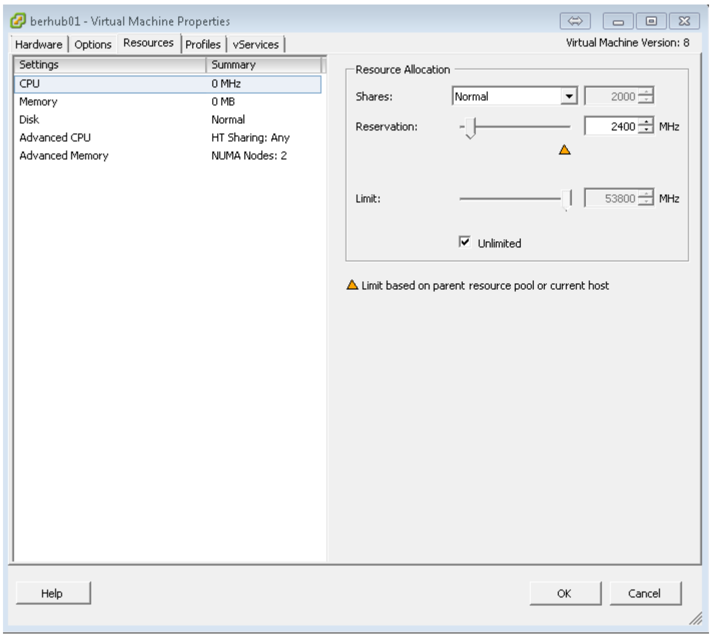
Please refer to your system requirements and documentation of your VMware server in advance. BluStar Server has been tested and is supported for version VMware vSphere V 5.1 and higher. The system requirements for running a BluStar Server apply also to a virtual machine, in terms of required operating system, hard disk space and additional supportive software. Please note that it is important for minimum latency of the BluStar Server to tie the resources of the virtual machine hosting the BluStar Server to the virtual machine for avoiding the actual resources / performance falling below the recommended system requirements.

3.6.2 VMware: Installation notes

It is recommended to deactivate the option for the CPU to go into the “C State” (core-parking). When creating a virtual machine using as a BluStar Server ensure the following CPU and memory resources:

3.6.3 VMware: CPU Resources

Set Shares to *Normal*, reserve at least *2200 MHz* and set limit to *Unlimited*.



Virtual Machine Version: 8

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Resource Allocation

Shares: Normal 2000

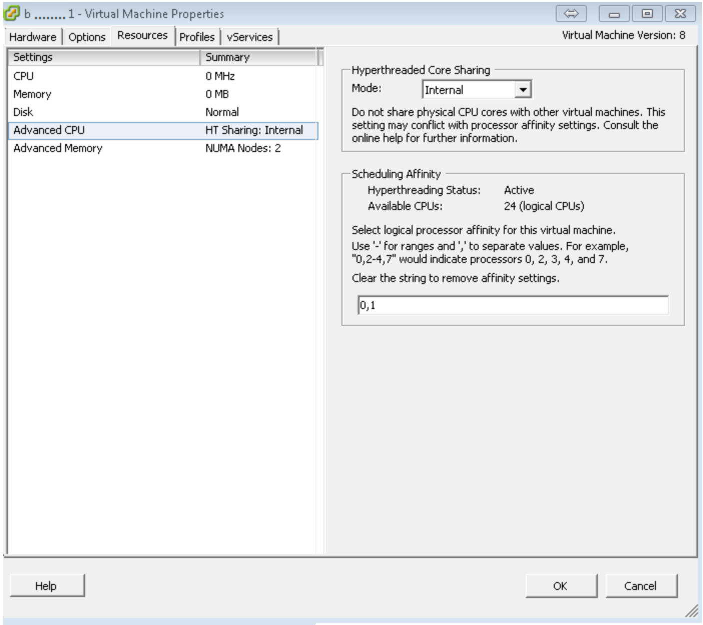
Reservation: 2400 MHz

Limit: 53800 MHz

☑ Unlimited

Limit based on parent resource pool or current host

It is strongly recommended to set the CPU affinity to at least two CPU cores used exclusively (“Hyperthreaded Core Sharing Mode”: “Internal”, “Scheduling Affinity” to two dedicated cores (i.e.”0, 1” or 4, 5 – dependent on the VMware host capabilities).



Virtual Machine Version: 8

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Internal
Advanced Memory	NUMA Nodes: 2

Hyperthreaded Core Sharing

Mode: Internal

Do not share physical CPU cores with other virtual machines. This setting may conflict with processor affinity settings. Consult the online help for further information.

Scheduling Affinity

Hyperthreading Status: Active

Available CPUs: 24 (logical CPUs)

Select logical processor affinity for this virtual machine.

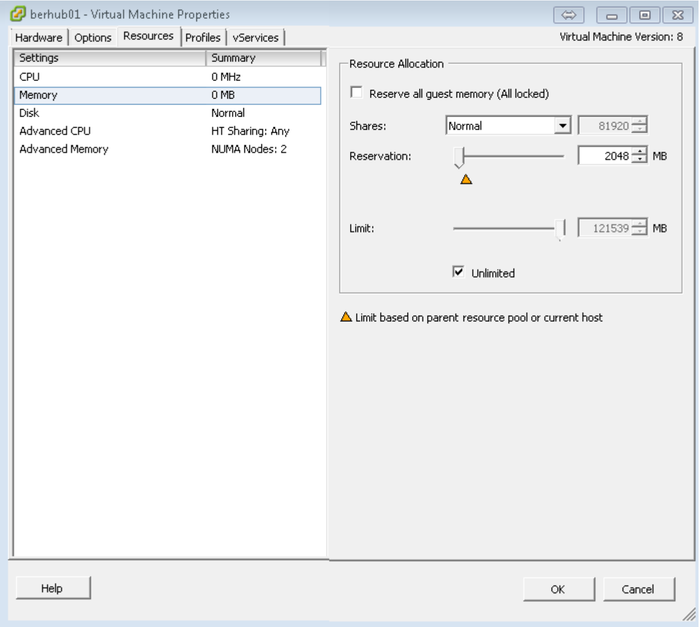
Use '-' for ranges and ',' to separate values. For example, "0,2-4,7" would indicate processors 0, 2, 3, 4, and 7.

Clear the string to remove affinity settings.

0,1

3.6.4 VMware: Memory Resources

Set Shares to *Normal*, reserve at least *2048 MB* and set limit to *Unlimited*. The recommendation is to increase this value if performance issues are encountered.


berhub01 - Virtual Machine Properties
Hardware
Options
Resources
Profiles
vServices
Virtual Machine Version: 8
Help
OK
Cancel

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Resource Allocation

□ Reserve all guest memory (All locked)

Shares: Normal 81920

Reservation: 2048 MB

Limit: 121539 MB

☑ Unlimited

Limit based on parent resource pool or current host

Extend the specific resource pool if you plan to add one or more virtual BluStar Servers to this pool.

3.6.5 Other VMware features

VMware HA (high availability) is not supported and doesn't guarantee seamlessly operation of the BluStar Server.
VMotion, moving a virtual machine to another vSphere server while running, is not supported.

3.7 Required information before starting the installation

Before the installation is started all required information should be available. An overview with all information that might be required for the installation is provided on the next page for reference. Depending on the installation, different data especially for the Presence Server are required. Please refer to the Presence Server chapter in this document for details.

BluStar Server installation

BluStar server:	
IP-address:	
DNS name:	
Administrator user name:	
Administrator password:	

Database:	
Control Data :	
Server name (including instance, e.g. BluStarServer01\SQLExpress):	
Database user (sa):	
Password:	

Call manager				
Type:	❑ MiVoice Office 400	❑ MiVoice /MX-ONE	❑ MiVoice 5000	❑ Other
Server name or IP address:				
Username (if required):				
Password (if required):				

Aastra directory LDAP import	
Server name:	
User name:	
Password	
Domain	
Search base	

Aastra directory Text import	
File name:	
Attributes (order of the attributes in the file)	

Connection to Microsoft Exchange	
Server name:	
User name:	
Password:	
Domain:	

Connection to Microsoft Lync	
Server name:	
User URL:	
Application name:	
Application port:	
ServiceGruu:	
Certificate name:	

3.8 Installation procedure

Installation Order – Overview

Step	Procedure
1	Configure the PBX and the PBX connection (e.g. MX-ONE)
2	Install the BluStar Server
3	Configure the BluStar Server (Chapter 0)

Step 1 – Configure the PBX and the PBX connection

Depending on the PBX which is to be used, different actions are necessary on different PBX's.
On some PBX's a specific user must be defined to be used by the CTI Server component of the BluStar Server to connect to the PBX.
Please note that appropriate licenses have to be implemented on the PBX, too.

Notice
Consult the appropriate PBX documentation for details of the configuration for the link to the BluStar Server and appropriate licenses required

Step 2 – Install the BluStar Server

This section briefly describes BluStar Server installation dialogs which are in fact more specific.
For other dialogs in the setup it is recommended to use the default answers and settings.
In the first specific dialog you can choose the installation type: Default (Single server installation) or Custom.
The feature tree dialog is only shown when performing a custom server installation. Here you can select which modules you want to install, it can be therefore used to distribute components to different servers.
In the next dialog the installation path can be changed (custom server installation).
In the next step a PBX can be selected and necessary connection parameters can be configured.
In the next dialog it must be selected if Microsoft SQL Server 2012 Express shall be installed on the machine locally or if an external Microsoft SQL 2005 / 2008 / 2012 server shall be used. If you installed Microsoft Windows following the guidelines in chapter 3.5, select to use an external SQL instance.

- If the installation of Microsoft SQL Server 2012 Express on the local machine is selected the installation routine will prompt for the password of the SQL 'sa' user account.
  This option is recommended for most installations.
- For using an external SQL server please refer to chapter 8.2 for details. The installation routine will ask for SQL server, the SQL username and the SQL user password.
  On a dedicated Microsoft SQL server the SQL authentication is to be used. If another user than 'sa' user should be used, please make sure this specific user has appropriate roles and rights.

Notice
Be aware that if Microsoft SQL Express is installed during the BluStar Server installation, the installation may fail especially when the server is in a Windows domain due to username / password policies.
The BluStar Server installation routine tries to apply changes to the IIS configuration to implement the web services for the administration of the BluStar Server which may fail for similar reasons.
Recommended actions in such case:

- Revert the installation of the BluStar Server (see chapter 9 for details)
- install Microsoft SQL Express manually (start “SQLEXPR_2012_x64.exe”. provided in the “x64 directory of the BluStar Server installation package) and make sure the password for the SQL-admin “sa” entered during the installation is matches the password complexity requirements of the Windows Domain. Make sure you install SQL Express in ‘mixed mode’. This is to make sure you set the ‘sa’ password.
- Install the BluStar Server but select the option to refer to an existing SQL server instead of installing the MS-SQL Express

After the type of database was selected the setup routine will start copying and installing the required software components. The components listed in chapter 3.5 are mandatory and have to be installed before launching the setup.
At the end of the copying and installation procedure the Aastra configuration database will be created. No further installation is required.

4 Configuration

For BluStar Server configuration open the BluStar Web Administration tool (http://<servername>/webadmin) with Microsoft Internet Explorer 9.0 or higher. Use the hostname or IP address of the computer where IIS with the Web Administration Application is installed.
The default user ID for administration is “admin” with password “Aastra123”. The password can be changed from the Web Administration GUI.

Configuration Order – Overview

Step	Procedure
1	PBX link configuration
2	Special CTI Server configuration – optional, not recommended to change
3	LDAP Server / Directory Sources configuration
4	Presence Server / Calendar Source configuration
5	Test the system

5 Step 1 – PBX link configuration

A connection to a communication server is called “PBX link”. Multiple PBX links may be handled by the BluStar Server simultaneously, i.e. for installations having multiple offices with separate communication servers. The PBX link is required i.e. for fetching line state information.

Menu: CTI Server → PBX links
The “PBX links” view displays all configured links to various servers and PBX’s.

The PBX link configuration can be viewed or changed (if the link is stopped) by clicking on the PBX link’s name.
When the data to connect to a communication server is provided during the installation, one link to the communication server will be established after the installation of the BluStar Server.

5.1 Add / configure a PBX link

Menu: CTI Server → PBX links
The configuration of a PBX link depends on the communication server used, the PBX interface respectively.

Link type	Communication server model
CSTA, direct connection	MiVoice Office 400, Aastra 5000, Aastra 700/Aastra MX-ONE

For detailed configuration click on the name of the PBX link. On the left hand side (navigation) the appropriate category must be selected.
If a new link is to be added, select: [Add PBX link]

Menu: CTI Server → PBX links → PBX link configuration
When adding a PBX link the properties of the new link are entered

Parameter	Explanation
PBX link name	Specify a name for this connection
PBX link number	This is generated by the server when saving the configuration
Server	This shows the available servers

Menu: CTI Server → PBX links → PBX link configuration → Telephone system

Parameter	Explanation
Telephone system	Select from the list the type of PBX
PBX connection	Direct connection is only available
Recognition external / internal numbers	Explicit / Implicit public: PBX sends a flag to differ the numbers DeviceIDs DeviceID length Prefix
Value	DeviceID length: Enter the maximum internal device number length + 1 Prefix: external numbers are recognized by the defined value at the beginning of the number
Handling of the outgoing numbers	Prefix which is appended by the CTI server for numbers of outbound calls

Handling of the incoming numbers	Prefix which is appended by the BluStar Server for numbers of incoming calls

Menu: CTI Server → PBX links → PBX link configuration → Telephony

Parameter	Explanation
External line prefix	Prefix for external extension numbers
Area code prefix	Prefix of the area code, e.g. “0” if area code is “0711”.
Area code	Area code for the current location
Used extension number block	Sequence of numbers from devices running on this link, if the devices have no link number
Extended device checking	To recognize hanging calls on the server if there are no more calls available
Host Prefix	Can be used to select multiple PBX with the same device number ranges with a unique prefix.

Menu: CTI Server → PBX links → PBX link configuration → Direct connection
The TCP/IP parameters like IP address of the PBX, port and password for the CSTA connection to the PBX are configured here. Actual data to be entered depends on the Telephone system selected.

Menu: CTI Server → PBX links → PBX link configuration → Number alignment
This feature can be used translate incoming numbers to a different outgoing number. Sometimes, PBX’s send a device number (e.g. 123) but need to be connected to a different number (e.g. 456). This could be if the wanted number is already used in the PBX, so another number is sent and needs to be translated.

Parameter	Explanation
Incoming	Received number from the PBX
Outgoing	Translated number to be dialed.

Notice
This feature could be risky to use. If errors are made in this list, it might be difficult to detect why certain users are not reachable.
Use this feature only if no other solution is available!

Menu: CTI Server → Monitors
Menu: CTI Server → CSTA messages
Menu: CTI Server → Server messages

The Menus can be used to check / supervise the status of an instance monitoring a specific extension and the messages for the PBX link / the CTI Server connection. Traces can be watched in order to log the CSTA traffic between CTI Server component and PBX, which may be useful for troubleshooting purpose.

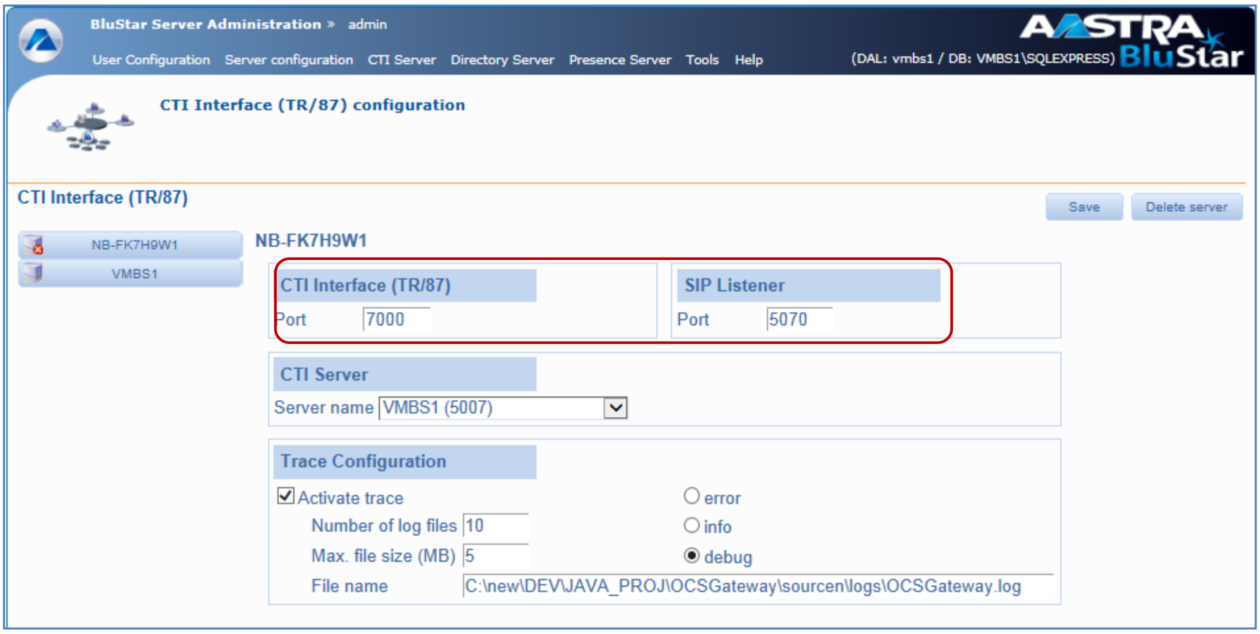
Extensions don’t have to be added manually to be monitored by the Presence Server later in the Monitors view, monitoring of the extensions will be requested automatically by the Presence Server.

5.2 Step 2 (optional) – Special CTI Server configuration

Menu: CTI Server → Configuration
The granularity of the messages on the server messages page for displaying trace messages on screen.

Network parameter for the DAL server the CTI server is connected to – not recommended for change.

Menu: CTI Server → CTI Interface



NB-FK7H9W1

CTI Interface (TR/87)
Port 7000

SIP Listener
Port 5070

CTI Server
Server name VMBS1 (5007)

Trace Configuration
☑ Activate trace
Number of log files 10
Max. file size (MB) 5
File name C:\new\DEV\JAVA_PROJ\OCSGateway\sourcen\logs\OCSGateway.log
○ error
○ info
● debug

Defining the CTI interface using TR/87 requires the use of port 5070 to be able to listen to the SIP messages as this is actually a SIP connecting used to transmit the CTI messages.

5.3 Step 3 – Directory Server configuration

This chapter describes the configuration of the Directory Server component of the BluStar Server. Keep in mind that the BluStar Server does not contain its own directory (aside from CSV-files stored locally for enhancing “higher authority directories” with entries which are e.g. typically not in an AD such as phones on floors, in server rooms, etc.). The BluStar Server reads the content of higher authorities’ LDAP server and / or AD and presents the results to the BluStar clients offloading mentioned “source servers”. The import from such “source servers” can be automated and scheduled for times with low traffic / low load conditions.

Take care not to install the BluStar Directory Server instance on the same server together with another LDAP Server like MS Active Directory – otherwise you have to specify a different port because the LDAP default port 389 may already be in use.

5.3.1 LDAP Server details

Menu: Directory Server → Configuration → LDAP Server
In the navigation section on the left the respective "source Server" can be selected and the appropriate configuration for the BluStar Server to access the "source servers" must be provided.

Settings:

Parameter	Explanation
Current suffix	Base DN (default: "dc=aastra, dc=com"). Once "Save" is clicked the BluStar Server will ask for confirmation since the (cached) database will be reset and all existing data will be deleted from the cache of the BluStar Server.
Port number	TCP/IP port for the LDAP server of the BluStar Server (default: 389)
Size limit of search	Maximal number of search results returned

Logging

Parameter	Explanation
Active	Enables / disables logging of the LDAP server component of the BluStar Server
Status Mode	Only status messages should be logged
Debug Mode	Status and debug messages should be logged
Log file size (Kbyte)	Maximum file size used for log files (default: 4000 kB)
Number of log files	Number of log files used (will be overridden / re-used once the maximum is exceeded).

Important
Logging in Debug Mode should only be activated temporarily to create detailed logs for a specific issue.
Logging in Debug Mode can influence the performance of the LDAP Server and should therefore be deactivated after the logs were created!

Delete/Write access

User / DN/Password	Credentials for delete/write access to the Directory Server component of the BluStar Server

Link-Button “More…” (available for multi-server installations only, for single server installations mentioned options can be accessed from the navigation bar on the left directly)
This button will open up more options in the navigator menu to the left for

- ASCII Import (note, there are 2 tabs)
- LDAP Import (note, there are 3 tabs)
- Attributes
- Index
- Import Status

5.3.2 ASCII / CSV import details

Menu: Directory Server → Configuration → ASCII Import
ASCII files with delimiters also known as “CSV files” can be imported to the BluStar Server database for being able to find i.e. extensions which do not exist in higher authorities’ databases like AD, i.e. phones on floors, in server rooms, etc.
The ASCII / CSV file may contain a first line containing column descriptions for the file but the BluStar Server just refers to the number of the column, thus the first line may have to be ignored when importing the file. (use the configuration option “Row(s) containing no data”)

Example for a file structure (1st line to be ignored, is just descriptive):
cn;sn;givenName;streetAddress;postalCode;postalAddress;telephoneNumber;homePhone;mobileTelephoneNumber;mail;facsimile;company;department;sipAddress
Anabelle Duck;Duck;Anabelle;;;;4711;;;anabelle.duck@noreply.com;;;;
Berta Duck;Duck;Berta;;;;4712;;;berta.duck@noreply.com;;;;
Willi Duck;Duck;Willi;;;;4223;;;willi.duck@noreply.com;;;;

When importing an ASCII / CSV file the BluStar Server ignores blanks between delimiters and it is also agnostic to CR or CF/LF delimiters at the end of each line. Thus the second example file (below) will lead to the same result when imported as the first example above:
cn; sn; givenName; streetAddress; postalCode; postalAddress; telephoneNumber; homePhone; mobileTelephoneNumber; mail; facsimile; company; department; sipAddress
Anabelle Duck; Duck; Anabelle; ; ; ; 4711; ; ; anabelle.duck@noreply.com; ; ; ;
Berta Duck; Duck; Berta; ; ; ; 4712; ; ; berta.duck@noreply.com; ; ; ;
Willi Duck; Duck; Willi; ; ; ; 4223; ; ; willi.duck@noreply.com; ; ; ;

Menu: Directory Server → Configuration → ASCII Import → ASCII import settings (1st tab)

Parameter	Explanation
Profile is active	Enables / disables the ASCII Auto import
Multi file support	Enables “multi file support” for up to 5 different import files
File path and name	Enter the file path and file name for the file containing data to be imported.
Limiting character	The character delimiter used for separating the columns
Row(s) containing no data	Enter the number of row(s) at the beginning of the file which shall be skipped during import
Overwrite / Delete old entries, Full database reset	Defines how to handle old entries when importing from a file
Allow duplicate entries	Allow duplicate entries where the first name, last name, company and department are the same.

Auto import

Configures scheduled import. Specify time of day, the day(s) of the week for automated import

Import rollback

Parameter	Explanation
No import verification	Disable checking the minimum number of entries imported
Minimum numbers of entries to import	Check the minimum number of entries imported. If the minimum number is not exceeded, the import will be invalid and no change to the database will be committed

Menu: Directory Server → Configuration → ASCII Import → ASCII import attributes (2nd tab):

Parameter	Explanation
Position in the file	Allows storing the imported data into favored fields, the position of the corresponding column within a row has to be mapped to the LDAP attributes.
Custom attributes	Assign imported columns to custom LDAP attributes. Enter the position in the file and mark the checkbox of the custom LDAP attribute.

5.3.3 LDAP Import details

Menu: Directory Server → Configuration → LDAP Import
LDAP sources can be i.e. OpenLDAP servers, the LDAP server of MiVoice Office 400 or others.

Menu: Directory Server → Configuration → LDAP Import → LDAP import settings (1st tab)
The Activate button activates the LDAP Auto import feature.

LDAP import settings

Parameter	Explanation
Profile is active	Shows the status of the Auto Import
Overwrite entries, Delete old entries and Full database reset:	Define how to handle old entries when importing from LDAP sources
Allow duplicate entries	Allow duplicate entries where the first name, last name, company and department are the same.

Auto import
Configures scheduled import. Specify time of day, the day(s) of the week for automated import. It is also possible to import the ASCII import at the same time.

Import rollback

Parameter	Explanation
No import verification	Do not check the minimum number of entries imported
Minimum numbers of entries to import	Check the minimum number of entries imported. If the minimum number is not exceeded, the import will be invalid and no change to the database will be committed

Menu: Directory Server → Configuration → LDAP Import → LDAP import server settings (2nd tab)
Server settings

Parameter	Explanation
Server	Name or IP address of the LDAP server the data shall be imported from.
Port	TCP port for doing LDAP connection.
Search bases	Position in the directory structure where LDAP bind is done.
Alternative import filter	LDAP import filter
Enable ‘Paged import’	Activate for executing a paged import (e.g. used for Active Directory imports, LDAP v3 is needed on the LDAP Server).
LDAP scope	Subtree or Onelevel

Login

Parameter	Explanation
Select the type of the LDAP login	Anonymous, With user information, User and domain (ADS).
Username	LDAP DN with access rights
Password	Password required for access the remote LDAP source
Domain	Enter an ADS domain.

Menu: Directory Server → Configuration → LDAP Import → LDAP import attributes(3rd tab)

Parameter	Explanation
Corresponding attributes	For importing data from another LDAP data base the attributes of the remote LDAP servers have to be assigned to the attributes of the Aastra LDAP server. Using “<xyz>” fixed values can be used.

Custom attributes	Maps custom LDAP attributes for the import. Example: Source attribute: businessCategory, target attribute: monitorGroup where monitorGroup is a custom attribute.

5.3.4 Export options details

Menu: Directory Server → Configuration → Export

As the BluStar Server collects directory information from various sources it may be desirable to let the BluStar Server dump its cached directory information gathered from mentioned sources; this is the purpose of the Export function.

Export settings

Parameter	Explanation
Profile is active	Enables /disables the export
File path and name	Enter the file name and file path to export the data to
Create header in export file	Enable first line in the file to contain the column names
Export all entries	Export all entries from the LDAP server (complete export)
Export only entries of the following organization	Limit the export to a specific organization. Example: Aastra Deutschland GmbH.

Auto export

Configures scheduled export. Specify time of day, the day(s) of the week for automated export.

Custom attributes

Parameter	Explanation
Target attribute	Enables custom attributes from the LDAP server to be exported

5.3.5 Attributes

Menu: Directory Server → Configuration → Attributes

Specifies custom LDAP attributes for the import/export.
Example: monitorGroup is a custom LDAP attribute which is a target attribute for LDAP import to which a source LDAP attribute businessCategory is mapped.

5.3.6 Index

Menu: Directory Server → Configuration → Index

More LDAP attributes to be indexed in order to accelerate the search within the LDAP server must be specified here. Changing this option is not recommended for administrators inexperienced with BluStar Server performance tuning.

5.3.7 Import Status

Menu: Directory Server → Configuration → Import Status
Manual import of ASCII files or LDAP data to the LDAP component of the BluStar Server and manual exporting data to an ASCII file. The current configuration of LDAP or ASCII (see above) is used.
A message window will show the status of the current automatic / manual import / export.
To update the messages displayed press the “refresh button” of the web browser to reload the page or enable the automatic refresh view option.

5.4 Step 4 – Presence Server configuration

Menu: Presence server → Configuration
The BluStar Server can aggregate presence information from Microsoft Exchange, Microsoft Lync 2013 as well as line state information from the PBX and provides it to the BluStar endpoints for the subscriptions (= all contacts located on the Home / Favorites screen) as well as when clicking on a directory query result. Similar as for the directory the BluStar Server offloads the calendar system from having many calendar subscriptions from every BluStar client.

> Notice
> To get access to presence services the configuration of a directory including the corresponding email AND SIP-addresses is mandatory. Without correctly configured directory the presence integration is not available as users do subscribe to the presence server using email address / SIP address and extension (telephone number). The BluStar Server is aggregating different presence information using the email address / SIP address/extension as a unique key. Search results entries with no valid email address or SIP address will be shown as “unknown” as it is not possible to get any presence information.
> It is recommended to use the default LDAP database with default settings (see 5.4.5)

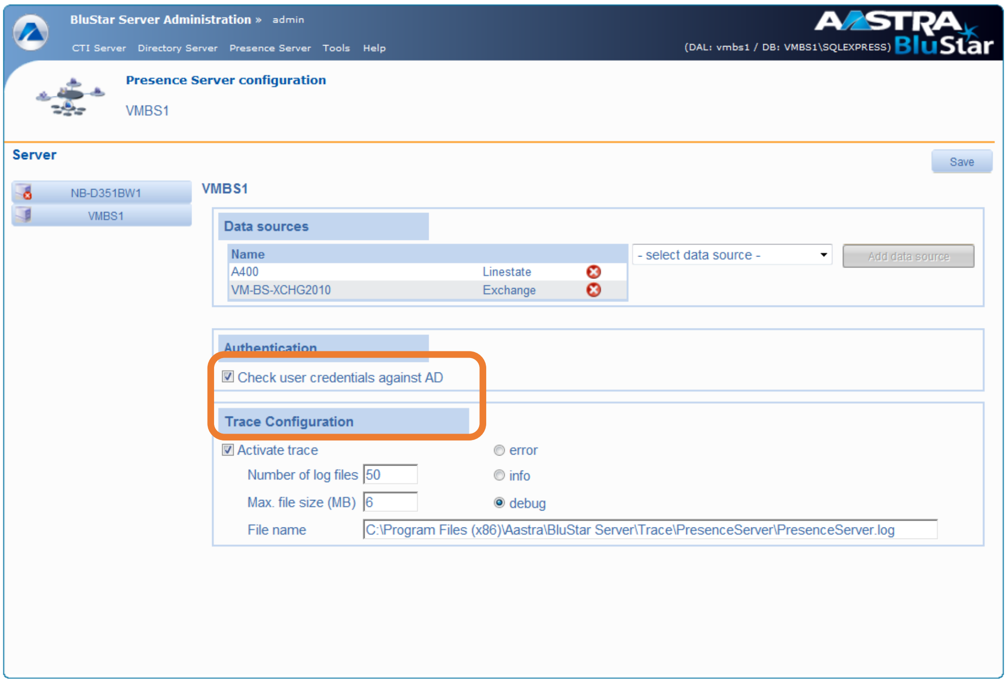
The following parameters must be configured on this page:

- “Data sources” for the Presence Server component of the BluStar Server. In the following pages the different databases must be configured for Exchange (Calendar) and line state. For exchange data source the refresh period can be configured for every calendar source individually. It is possible to define a time offset to let the BluStar Server modifying the times for calendar entries if the default value is not applicable; e.g. if the BluStar Server is located in a time zone different from the calendar server.
- Authentication; enables or disables authentication of users AD credentials when subscribing for presence.
- Trace Configuration data: Activates or deactivates tracing of the Presence Server component of the BluStar Server and allows selection of the trace level (error, info or debug). The location and file name of the trace file and the number of log files and their maximum size can be defined as well

Notice

For subscribing to the presence of users and for publishing presence status, the user must provide its AD credentials to the BSCpc / BSCiOS. Both values – username and password – will be stored in encrypted format in the file system of the respective device (if the respective checkbox is "checked"). Credentials are transferred to the BluStar Server in encrypted format and the BluStar Server checks in AD if the data matches to a user. If so, the user is allowed to publish / subscribe presence.

The administrator may decide NOT to force BSC's to authenticate against AD.



(DAL: vmbs1 / DB: VMBS1\SQLEXPRESS)

Presence Server configuration

VMBS1

Server

NB-D351BW1

VMBS1

Save

VMBS1

Data sources

Name		
A400	Linestate	⊗
VM-BS-XCHG2010	Exchange	⊗

- select data source -

Add data source

Authentication

☑ Check user credentials against AD

Trace Configuration

☑ Activate trace

Number of log files: 50

Max. file size (MB): 6

File name: C:\Program Files (x86)\Aastra\BluStar Server\Trace\PresenceServer\PresenceServer.log

○ error
○ info
● debug

Notice

BluStar Server is mapping some free text entries to translated strings (all supported client languages).

This mapping is hardcoded and not configurable.

These preconfigured strings are:

available
busy
unavailable
signed out
in a meeting
in a call
be right back
away

5.4.1 Line state configuration details for the Presence Server component

Menu: Presence server → Configuration
The line state considered in the Presence Server component of the BluStar Server is requested from the CTI Server component of the BluStar Server. The CTI Server component handles the PBX links (see CTI Server → PBX links).

The CTI Server component of the BluStar Server is a "Data source" for the Presence Server component of the BluStar Server like i.e. MS-Exchange calendars; thus the CTI-Server component of the BluStar Server must be added as a "Data source" as well ("Add data source", type: "Linestate").

Please note that the "Data source(s)" to be added for line state information must be one of the installed / configured CTI Server components of the BluStar Server, also the port used must be the same as the one configured for the CTI Server component of the BluStar Server (Menu: CTI Server → Configuration).

Clicking on the link of the "Data source" name and on the "Advanced" button opens an options menu for line state details to be considered by the Presence Server component of the BluStar Server:

Menu: Presence server → Configuration → Linestate (link)

Parameter	Explanation
Data source name	Each data source must be assigned an alias which is unique in the Presence Server configuration
Device	Enter a valid extension number to test the connection

Connection data

Parameter	Explanation
Server name	The hostname or IP address of the CTI Server
Port	The port of the CTI Server (default 5077)
Backup server	The hostname or IP address of the backup CTI Server.
Port	The port of the backup CTI Server (default 5077)

Each data source must be assigned an alias that is unique in the Presence Server configuration.

- primary connection / server name / port
- backup server (when available) / server name / port (optional, not required for single server installations)

Usually the BluStar Server will retrieve all line states from the PBX's and no specific configuration on the advanced settings is required.
There are certain scenarios for which it is helpful to define restrictions using ranges, patterns and prefixes. Restrictions are specifically useful

- to exclude specific extensions from being monitored
- when having more than one PBX link but PBXs host the same extension number (i.e. 100 may exist on PBX 1 and on PBX 2), thus the Restrictions may be used to filter by prefix (area code or PBX main number) to route the line state requests to the appropriate PBX

link (the option “use specific domain / link” shall be used to identify the PBX links ID to be used for routing the line state requests to the appropriate PBX)

With “Range“, “Prefix” and “Pattern” the devices / extensions are defined for which the line state is to be retrieved. It is also possible to configure a combination of one or more restrictions. The configured ranges, prefixes and patterns will be combined in a mathematical “and” rule, the different restrictions inside ranges, prefixes and patterns will be used in a mathematical “or” rule.

- If no restriction matches the extension number then line state will not be supported for this device/extension number.
- If no restrictions are defined then the Aastra Presence Server will try getting line state for every extension number.

Menu: Presence server → Configuration → Linestate (link) → Advanced

Connection data

Parameter	Explanation
Server name	The hostname or IP address of the CTI Server
Port	The port of the CTI Server (default 5077)
Backup server	The hostname or IP address of the backup CTI Server
Port	The port of the backup CTI Server (default 5077)

Range

Parameter	Explanation
From	The range of extension numbers that starts from this value Example: 300 - 400
To	The range of extension numbers that ends from this value.

Prefix

Parameter	Explanation
Value (1…3)	The prefix of extension numbers that starts with this value. It is also possible to define a prefix like a company prefix. This means every extension number that starts with this prefix will be used for getting line state.
Delete (1…3)	Checkbox to enable removing of the prefix.

Pattern

Parameter	Explanation
	Pattern of extension numbers like “8xxx”, → all extension no’s starting with “8” having a length of 4 token will be handled

Domain/Link

Parameter	Explanation
Use specific domain/link	If multiple PBX links are used to connect to multiple communication servers the PBX link to be used for this specific data source can be identified by the number / index of the PBX link. The index can be found in CTI Server → PBX links, "PBX link No."

Please note that there is a button "Test connection" to validate the whole logical chain:
PBX line state interface → PBX link → CTI Server → Presence Server.
The "Test connection " button can be found in the menu
Presence Server → Configuration → click on a PBX link presented as "Data source"

It is recommended to use this test for validation the Range / Prefix / Pattern settings as well as the link to the PBX system. Please note that an inappropriate configuration may lead unwanted results such as delayed presence presentation on clients or "no line state" at all.

5.4.2 Exchange as calendar source – configuration details

Menu: Presence server → Configuration → Exchange server (link)

Parameter	Explanation
Data source name	Each data source must be assigned an alias which is unique in the Presence Server configuration
Email address	Enter a valid email address to test the connection

Connection data

Parameter	Explanation
Server name	The hostname or the IP address of the Exchange Server
Mail Domain	This the postfix (the string after @) of the email addresses
Username	This is the username of the Exchange user, which will be used to access all calendars for this configuration
Password	This is the password of the Exchange user
Domain	This is the windows domain of the Exchange Server

Access type

Parameter	Explanation
WebService(2007, 2010)	When using Microsoft Exchange Server 2007, 2010 or 2013, this radio button should be selected
Access protocol	Default is "https"
Authentication	Normally "Impersonation" will be used. When using Microsoft Exchange Online the option "Delegate" has to be used
Use notification service	Must be enabled when notification service "Aastra Presence Notification" should be used
WebDAV(2000,2003)	When using Microsoft Exchange Server 2000,or 2003, this radio button should be selected

Access protocol	Protocol to be used for the web access.
Virtual path	This is part of the context path. The value is by default “Exchange”, e.g. http://exchangeserver/Exchange/hans.test/calendar
Retrieving by	This is also part of the context path. Exchange 2003 uses by default the “User Name”, which is a prefix of the mail address. The URL looks like http://exchangeserver/exchange/hans.test/calendar
Remote Directories	This is a language specific value. This is part of the context path for calendar URL of the web access. E.g. http://exchangeserver/exchange/hans.test/calendar. Several values can be added by the combo box
Use autodiscover service	Used for integration with Microsoft Exchange Online / 365 to retrieve the assigned server for the user
Request URL / Event URL	These two URLs are passed to Exchange and are used by Exchange when changes on subscribed mail boxes occur

The visibility of the users’ calendar entries can be controlled by the BluStar Server administrator.
Menu: Presence Server → Configuration →Exchange Server → click “More”
All configuration applied is valid for all BluStar Server users, calendar owners and entities (meeting rooms, etc.) for which the calendar status is to be displayed.
It is here also that the update interval for calendar entries is configured together with a time offset to modify the time of calendar entries when the BluStar Server and Exchange server are in different time zones.
The categories of calendar entries to be published by the BluStar Server to Presence Clients can be selected (free, tentative, busy, out of office), this setting applies for “public” and “private” calendar entries.
By default calendar entries which are not marked as “private” are published with their details (“Subject” and “Location”). For improved privacy the details can be hidden or overridden by static text if the option “Override calendar entries’ properties by static text before publishing” is checked.
Calendar entries marked as “private” are not published to Presence Clients by default and are not considered for the status at all. To publish private calendar entries the check box “Publish ‘private’ calendar entries” must be selected; for enhanced privacy the “Subject” and “Location” of private calendar entries can be overridden by static text, too.
Please note: To override “Subject” or “Location” at least one character (not a blank!) must be provided, thus it is possible to leave the “Subject” unchanged but to hide the “Location” by using “-“ as static text for overriding the information.

5.4.3 Lync as presence source – configuration details

Menu: Presence server → Configuration → Lync (link)

Parameter	Explanation
Data source name	Each data source must be assigned an alias which is unique in the Presence Server configuration
SIP address	Enter a valid SIP address to test the connection
Presence federation (checkbox)	Enables the Presence Server to PUBLISH line state changes or BluStar presence changes towards Lync Users (Lync license required) via UCMA interface
Activate permanent subscriptions (checkbox)	can be used to have these subscriptions permanently independent from BluStar clients subscribing them (e.g. to federate line state of phones without active BluStar client)

Connection data

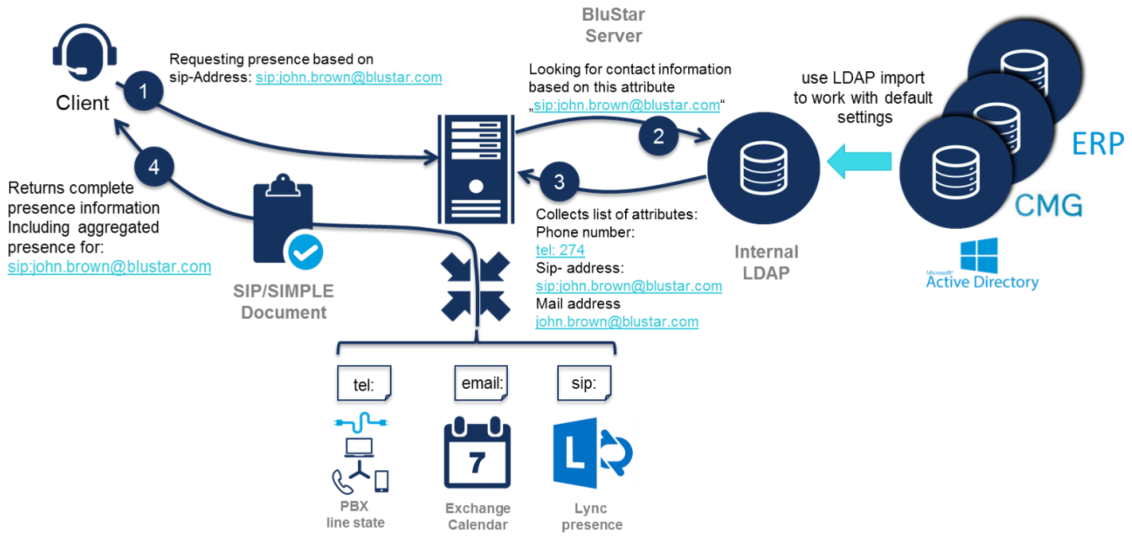
Parameter	Explanation
Server name	The FQDN of the Lync Server
SIP domain	This the postfix (the string after @) of the SIP addresses
User URI	This is a valid URI of the Lync user Necessary to identify the endpoint against the Lync Server
Application name	Name of the Trusted Application (details how to obtain this information see chapter 6.3 Microsoft Lync)
Application port	Port of the trusted Application (details how to obtain this information see chapter 6.3 Microsoft Lync)
Application user agent uri (GRUU)	Service Gruu of the Trusted Application (details how to obtain this information see chapter 6.3 Microsoft Lync)
Certificate name	Name of the certificate created for the BluStar Server

5.4.4 Presence Server Presence Interface configuration

To access directory data used for calendar and line state information you can configure the BluStar Presence Server in two ways.

1 - By default the internal BluStar directory server is defined as database. Based on an Open LDAP Server it provides features to import content from multiple/different source servers to be used with the BluStar Clients and the BluStar Presence Server.

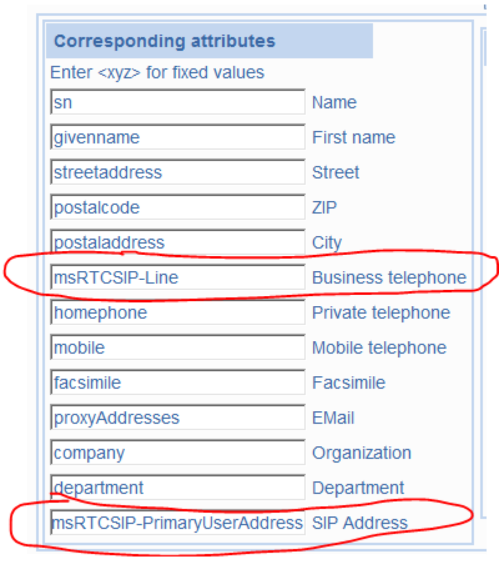
This configuration is recommended as you can merge different data sources to one and grant access to both, internal and external contacts without any additional load on the source systems and you can go with most of the default settings for presence configuration.


BluStar Server
Client
1
Requesting presence based on sip-Address: sip:john.brown@blustar.com
Looking for contact information based on this attribute „sip:john.brown@blustar.com“
2
use LDAP import to work with default settings
ERP
CMG
Active Directory
3
4
Returns complete presence information Including aggregated presence for: sip:john.brown@blustar.com
Collects list of attributes: Phone number: tel: 274 Sip- address: sip:john.brown@blustar.com Mail address john.brown@blustar.com
Internal LDAP
SIP/SIMPLE Document
tel:
email:
sip:
PBX line state
Exchange Calendar
Lync presence

By mapping AD attributes to default LDAP attributes on import you can always use the default presence interface configuration.

Sample: Microsoft Lync user attributes from Active Directory imported to default

“SIP Address” and “Business telephone”:



Corresponding attributes

Enter <xyz> for fixed values

sn	Name
givenname	First name
streetaddress	Street
postalcode	ZIP
postaladdress	City
msRTCSIP-Line	Business telephone
homephone	Private telephone
mobile	Mobile telephone
facsimile	Facsimile
proxyAddresses	EMail
company	Organization
department	Department
msRTCSIP-PrimaryUserAddress	SIP Address

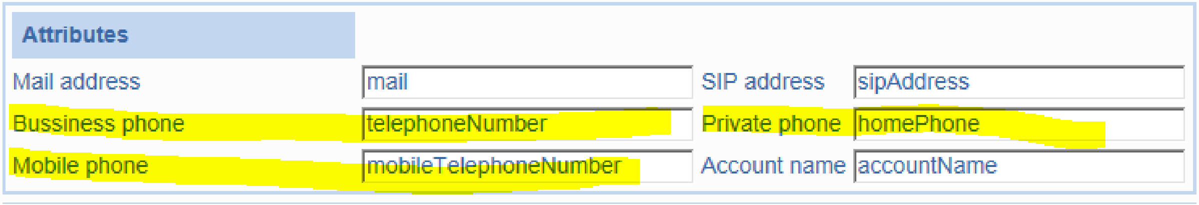
→ Directory Server / LDAP Import / LDAP Import attributes

Directory Configuration Default

Parameter	**Explanation**
Email	Enter a valid email address to test the connection
Default/Advanced	Choose **Default** to use the BluStar Directory Server data base, configuration settings as shown but are not configurable.

The LDAP database is optimized for high load and as indexed on phone number to be optimized for quick search operations. Therefore the use of this database should always be considered no matter which and how many external resources to connect to.

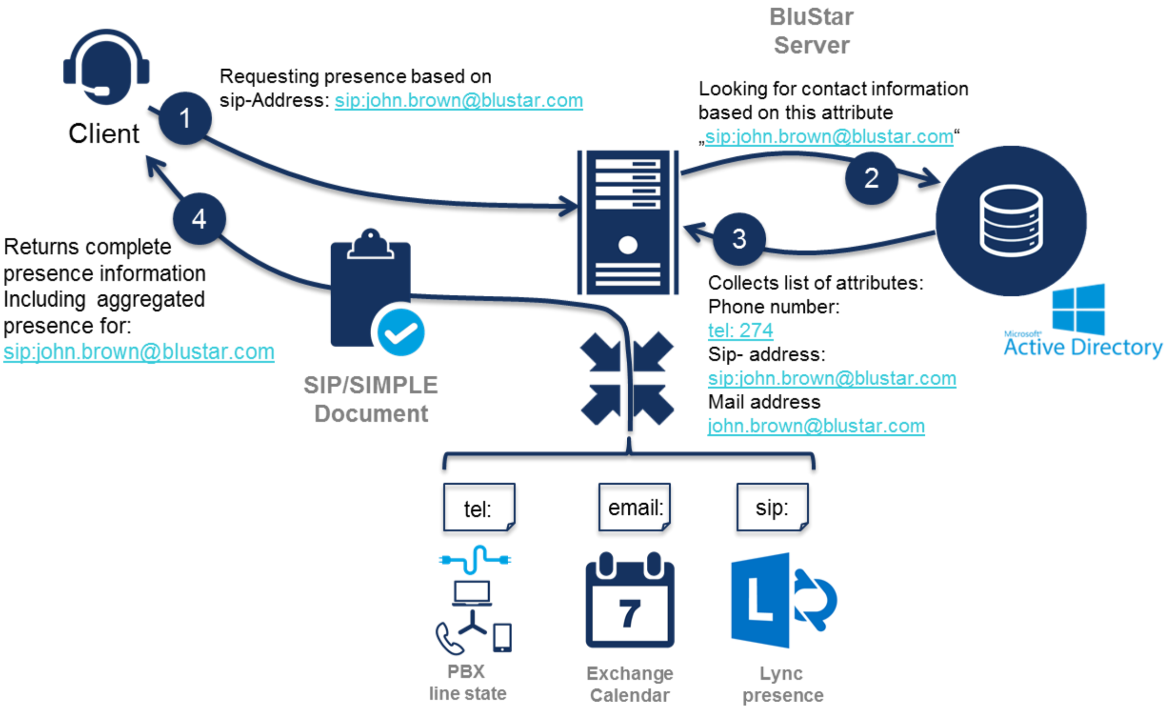
The Presence Server tries to fetch line state based on three Attributes configurable via WebAdmin→ Presence Interface Configuration:



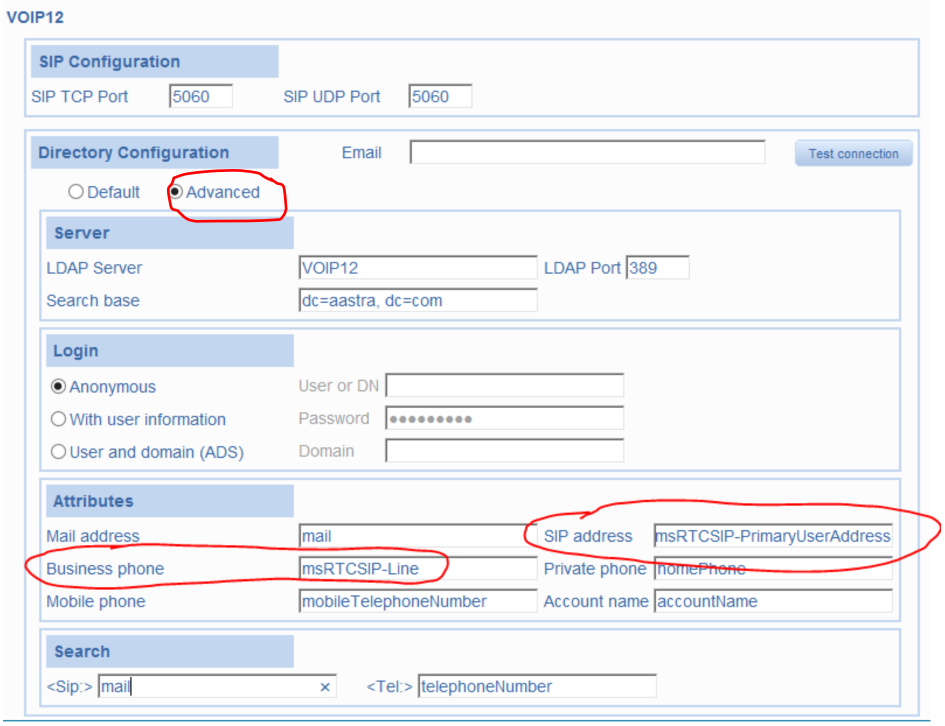
Attributes

Mail address	mail	SIP address	sipAddress
Bussiness phone	telephoneNumber	Private phone	homePhone
Mobile phone	mobileTelephoneNumber	Account name	accountName

2 - Optionally (not recommended) you can configure the BluStar Presence Server directly to connect to one external directory via LDAP e.g. Microsoft Active Directory.


BluStar Server
Client
1
Requesting presence based on sip-Address: sip:john.brown@blustar.com
Looking for contact information based on this attribute „sip:john.brown@blustar.com“
2
3
4
Returns complete presence information Including aggregated presence for: sip:john.brown@blustar.com
Collects list of attributes:
Phone number:
tel: 274
Sip- address:
sip:john.brown@blustar.com
Mail address
john.brown@blustar.com
Microsoft Active Directory
SIP/SIMPLE Document
tel:
email:
sip:
7
PBX line state
Exchange Calendar
Lync presence

In this case you usually will have to adjust the setting by using “Advances Settings” for the Presence Interface configuration:


VOIP12

SIP Configuration

SIP TCP Port 5060 SIP UDP Port 5060

Directory Configuration Email [ ] Test connection

○ Default ● Advanced

Server

LDAP Server VOIP12 LDAP Port 389

Search base dc=aastra, dc=com

Login

● Anonymous User or DN

○ With user information Password ●●●●●●●●●

○ User and domain (ADS) Domain

Attributes

Mail address	mail	SIP address	msRTCSIP-PrimaryUserAddress
Business phone	msRTCSIP-Line	Private phone	homePhone
Mobile phone	mobileTelephoneNumber	Account name	accountName

Search

<Sip:> mail × <Tel:> telephoneNumber

Be aware that in this configuration every directory activity of the Presence Server (e.g. each subscription) is a direct access to the external source.

Directory Configuration/Advanced

Parameter	Explanation
Email	Enter a valid email address to test the connection
Default/Advanced	Choose **Advanced** to configure an external data base like Microsoft Active Directory or Mitel CMG LDAP, configuration settings are configurable

Attributes	Explanation
Mail address	External LDAP data base attribute (e.g.mail)
Business phone	External LDAP data base attribute (e.g.telephoneNumber)
Mobile phone	External LDAP data base attribute (e.g.mobileTelephoneNumber))
SIP address	External LDAP data base attribute (e.g.sipAddress) In many cases (e.g. when using Mitel CMG LDAP or if Email sddress=SIP Address) *email* has to be / can be used to map email address to SIP address
Private phone	External LDAP data base attribute (e.g.homePhone)
Account name	External LDAP data base attribute (e.g.accountName)

Menu: Presence server → Presence Interface

SIP Configuration

Parameter	Explanation
SIP TCP Port	TCP port used for SIP SIMPLE (default 5060)
SIP UDP Port	UDP port used for SIP SIMPLE (default 5060)

Directory Configuration

Parameter	Explanation
Email	Enter a valid email address to test the connection
Default/Advanced	Choose Default to use the BluStar Directory Server data base, configuration settings as shown but are not configurable. Choose Advanced to configure an external data base, configuration settings are configurable

Directory Configuration/Advanced

Server

Parameter	Explanation
LDAP Server	The hostname or IP address of the LDAP Server
LDAP Port	TCP/IP port for the LDAP server
Search base	Base DN

Login

Parameter	Explanation
Anonymous/With user information/User and domain (ADS)	Select the login method
User or DN	Only required when With user information or User and domain (ADS) is selected
Password	Only required when With user information or User and domain (ADS) is selected
Domain	Only required when User and domain (ADS) is selected

Attributes

Parameter	Explanation
Mail address	External LDAP data base attribute (e.g.mail)
Business phone	External LDAP data base attribute (e.g.telephoneNumber)
Mobile phone	External LDAP data base attribute (e.g.mobileTelephoneNumber))
SIP address	External LDAP data base attribute (e.g.sipAddress)
Private phone	External LDAP data base attribute (e.g.homePhone)
Account name	External LDAP data base attribute (e.g.accountName)

Search

Parameter	Explanation
<Sip>	Search attribute in External LDAP database (e.g. mail)
<Tel>	Search attribute in External LDAP database (e.g. telephoneNumber)

5.5 Step 5 – Test the system

Assuming that the creation and the establishment of the CTI link in the previous step were successful the following steps can be used to verify the installation:
Login to the BluStar Server with a browser (address: http://IP-address-of-BluStar-Server/webadmin)

- Browse to the “monitoring view” (‘CTI Server → Monitors’) in the Web Administration tool
- Start a monitoring point for a specific extension
- Now initiate a call (inbound or outbound) on this extension
- Browse to the CSTA view (‘CTI Server → CSTA messages’) in the Web Administration tool

Some events logged for the monitored extension shall be visible now (browser will reload periodically).

6 Presence Server configuration requirements

The Aastra Presence Server component of the BluStar Server supports standard protocols to communicate with Microsoft Exchange Servers; thus no third party applications are required.
BluStar clients can subscribe calendars of specific users / contacts from Microsoft Exchange for receiving events when appointments are modified or getting active / inactive.
This chapter describes the configuration required on the Exchange Servers / Windows Server components for granting access to the BluStar Server to the Microsoft Exchange database.

In MITEL MCC it is required to configure Username and Password in order to authenticate for Presence.

For MITEL MCC there is a default Account/password configured.

- The default account is <comdasys_Mitel MCc>, the default password is <Aastra123>.
- The password can be changed within the BluStar Server Administration.

6.1 Presence Server configuration

Menu: Presence Server → Configuration
If the Presence Server component has started successfully, you can see this in the Web Administration tool; like for all other components of the BluStar Server the configuration for traces is predefined when the Presence Server component starts the first time.
All parameters for one or more data sources must be configured according to the description below.

6.2 Microsoft Exchange

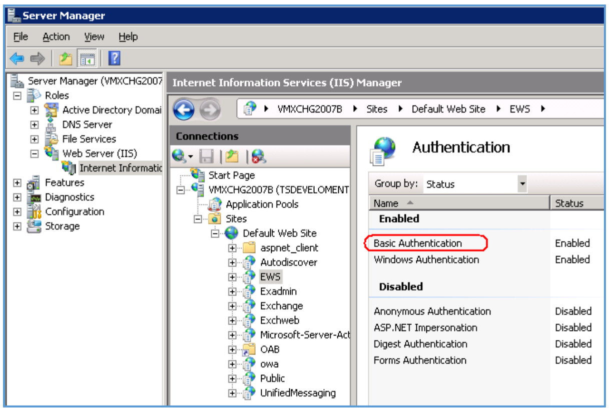
The Presence Server component of the BluStar Server supports the following versions of Microsoft Exchange:

- Exchange 2007 SP1
- Exchange 2010
- Exchange 2013
- Microsoft Exchange Online

To allow the BluStar Server connecting to the Microsoft Exchange server the Microsoft Exchange server must be configured appropriately; such configuration is described in the next chapters.
The WebService interface is available in Exchange Server 2007 and higher versions.

6.2.1 WebService: Windows Server 2008 (R2)

When using Windows Server 2008 the following “Basic Authentication” or “Windows Authentication” has to be added in the Server Manager:



Group by: Status

Name	Status
Enabled	
Basic Authentication	Enabled
Windows Authentication	Enabled
Disabled	
Anonymous Authentication	Disabled
ASP.NET Impersonation	Disabled
Digest Authentication	Disabled
Forms Authentication	Disabled

6.2.2 WebService: Exchange Server 2007 User Configuration

To use this interface to communicate with Microsoft Exchange Server 2007 the following parts have to be configured:

- For using WebService create a normal user (e.g. WebServiceAdmin) in Active Directory and create a mailbox for this user.
- Then assign the needed rights to this user. Open the Exchange Management Shell and execute the following commands:

```
Get-ExchangeServer | where {$_.IsClientAccessServer -eq $TRUE} | ForEach-Object
{Add-ADPermission -Identity $_.distinguishedname -User WebServiceAdmin -
extendedRight ms-Exch-EPI-Impersonation}
Get-MailboxDatabase | ForEach-Object {Add-ADPermission -Identity
$_.DistinguishedName -User WebServiceAdmin -ExtendedRights ms-Exch-EPI-May-
Impersonate}
```

6.2.3 Web Service: Exchange Server 2010 User Configuration

To use this interface to communicate with Microsoft Exchange Server 2010 the following parts have to be configured:

- For using Web Service create a normal user (e.g. WebServiceAdmin) in Active Directory and create a mailbox for this user.
- Then assign the needed rights to this user. Open the Exchange Management Shell and execute the following command:

```
New-ManagementRoleAssignment -Name:AastraAssignmentName -
Role:ApplicationImpersonation -User: WebServiceAdmin
```

Notice

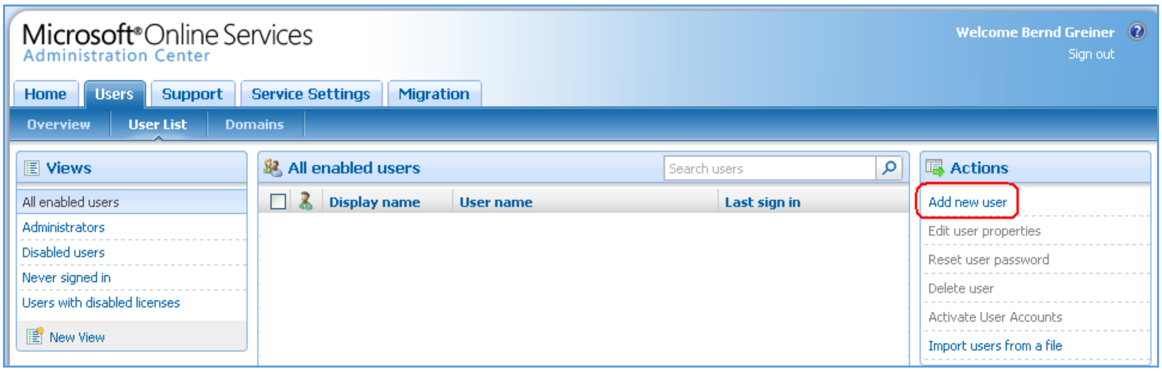
The name for the “New-ManagementRoleAssignment” is only a name; you can choose what you want. It is not referenced anywhere.

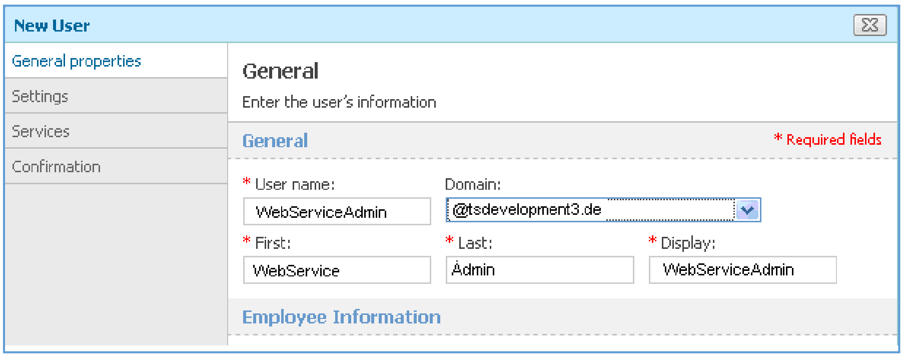
6.2.4 WebService: Microsoft Exchange Online

Microsoft Exchange Online is a Microsoft-hosted enterprise messaging service based on Microsoft Exchange Server 2007.

> Notice
> With Microsoft Exchange Online you have to create a user with administrator rights.

Create a user with the Administration Center in the Microsoft Online Services Administration page:





General

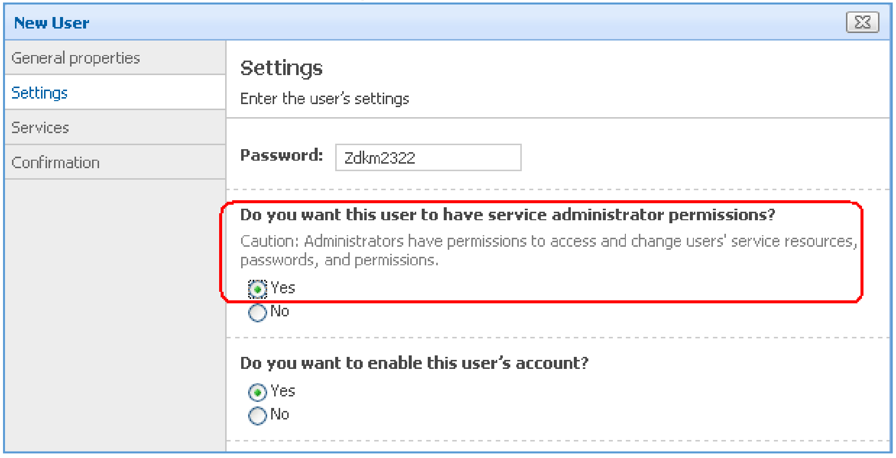
Enter the user's information

General * Required fields

* User name: WebServiceAdmin	Domain: @tsdevelopment3.de	
* First: WebService	* Last: Admin	* Display: WebServiceAdmin

Employee Information

This user needs administrator permissions.



Settings

Enter the user's settings

Password: Zdkm2322

Do you want this user to have service administrator permissions?

Caution: Administrators have permissions to access and change users' service resources, passwords, and permissions.

● Yes
○ No

Do you want to enable this user's account?

● Yes
○ No

After creating this user, open the Administration Center page again with the credentials of the new user to verify it exists and has appropriate access rights.

6.2.5 Configuration of the BluStar Server to access calendar for Presence

The base configuration has to be done at the “Data source” configuration. Note that the BluStar Server is able to connect to multiple Exchange servers simultaneously.
Each data source must be assigned an alias that is unique in the Presence Server component configuration of the BluStar Server.

Connection data

Provide the Exchange server name, the user credentials for the user account to access the Exchange server, the Mail domain then the Domain name (may equal to the mail domain name).

Server: The hostname (fully qualified) of the Exchange Server. If the DNS cannot resolve a given IP-address then add an entry in the local hosts file with IP-address and full qualified hostname.

Mail Domain: This the postfix (the string after @) of the email addresses. Here you add the data for the Exchange user you have configured for access to the Microsoft Exchange Calendars.

Username: This is the username of the user, which will be used to access all calendars for this configuration.

Notice
In some environments it is necessary to add the domain as a prefix of the user name like DOMAIN\USERNAME

Notice
When using Microsoft Exchange Online the mail address has to be used as username.

Password: This is the password of the user.

Domain: This is the domain of the user.

Notice
When using Microsoft Exchange Online the domain field remains empty.

6.2.6 Configuration of the BluStar Server for accessing the Exchange 2007, 2010, 2013 via Webservice

When using WebService the following settings are also enabled and have to be configured.

Access protocol

When using WebService the access protocol can be configured. The default is “https”. If “SSL” is not configured by the Exchange Server administrator “http” has to be used.

Authentication

“Impersonation” will be used as a default, only for Microsoft Exchange Online the “Delegate” has to be selected.

Using Notification Service

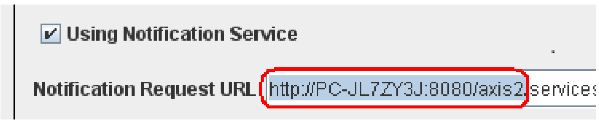
When using “Aastra Presence Notification” select the checkbox and make sure the service “Aastra Presence Notification” is started.

Notification Service
To get calendar events from MS Exchange via webserver there are two options:

1. BluStar Server polls actively all calendars of subscribed users.
   Update interval defined on page two of the presence server configuration.

2. Using notification Service - recommended:
   - no periodic poll towards Exchange server
   - BluStar Notification Service gets notification about calendar changes.
     Internally the Presence Server is polling the Notification Service (based on the time interval defined on configuration page two) for new information and then is fetching the changed content from Exchange actively.

Important
When using Notification Service then this service should be accessible from the Exchange Server.
Open a browser on the Exchange Server and request an URL like:
http://BLUSTAR_SERVER_HOST:8080/axis2
You will find this URL here:



☑ Using Notification Service

Notification Request URL http://PC-JL7ZY3J:8080/axis2 services

Maybe add a new entry in the hosts of the Exchange Server.

6.3 Microsoft Lync

Microsoft Lync will give you access to presence information, but with special functionality. The service will act as a presence server also updating presence information available on the BluStar Client in the Microsoft presence server.
First manually install the SDK from the media kit (<UcmaRuntimeSetup.exe>) and install the CA and Lync certificates before you define the link. A prerequisite for installing the UCMA SDK is the Server Feature “Media Foundation” which can be added using the Server Manager. The certificates need to be added to the <Local Computer> certificate store under “Trusted Root Certification Authorities”.

It can be useful to (temporary) install a Microsoft Lync client on the server for testing purposes. This way you can be sure the certificates are working properly.
Then check that the Lync client is up and running by changing the presence status in the client (not possible if Lync is not running correctly).

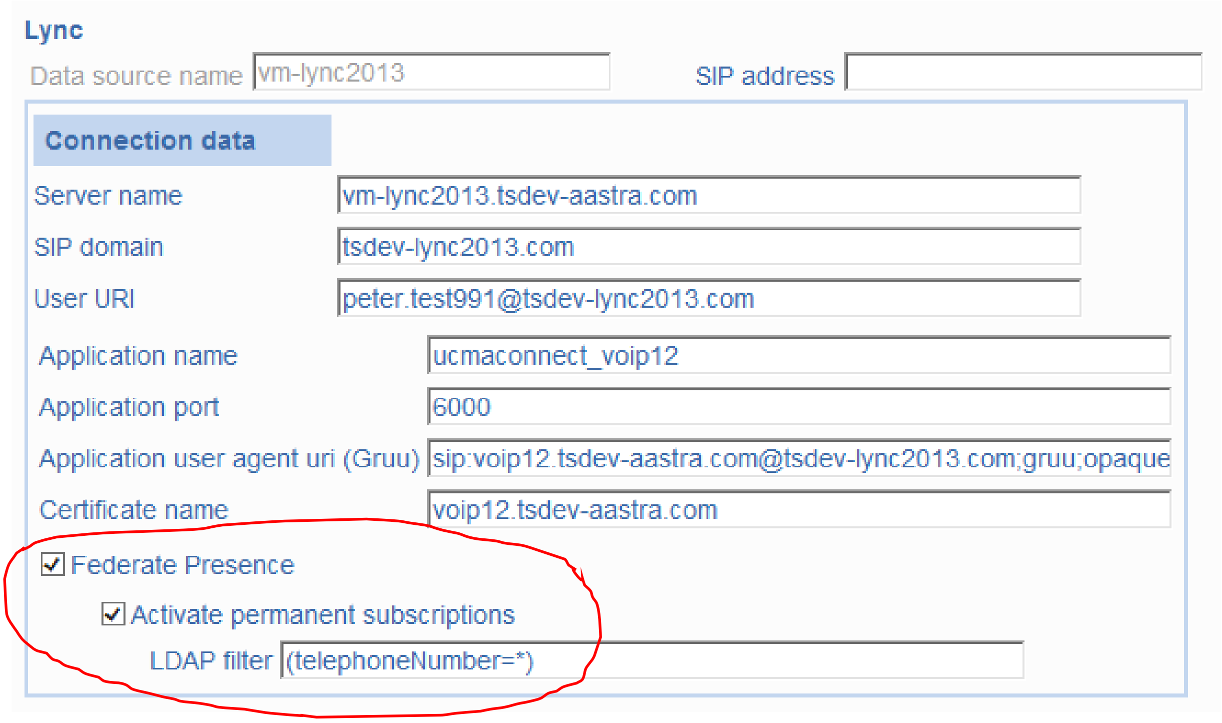
We expect that any integration with Microsoft Lync is performed only by persons who have appropriate training and experience in the configuration and administration of Lync systems.
It must be ensured that sufficient and correct licenses are installed on the Lync system for the intended use.
With “Federate Presence“ activated in the Presence Server configuration the BluStar Server will be enabled to PUBLISH e.g. line state changes towards Lync via UCMA interface.

- Line state example: if BluStar Server receives a busy event via CSTA he will publish “in a call” towards Lync
- BluStar Presence: changing the BluStar presence state via BluStar clients will result in a PUBLISH towards Lync using the corresponding Lync state

This will also work if the Lync client of the corresponding user is not started:

- The Lync user in a Lync favorite list may be grey (Offline), if the person is on a Mitel phone speaking it will turn to red “Busy-in a call” and after the call turn back again to grey/Offline.

If you want to use this feature for phones without a corresponding Lync Client installation “Activate permanent subscriptions” need to be activated for these devices. You will also need to order Lync federation licenses for the BluStar Server.



Lync

Data source name: vm-lync2013
SIP address:

Connection data

Server name: vm-lync2013.tsdev-aastra.com
SIP domain: tsdev-lync2013.com
User URI: peter.test991@tsdev-lync2013.com
Application name: ucmaconnect_voip12
Application port: 6000
Application user agent uri (Gruu): sip:voip12.tsdev-aastra.com@tsdev-lync2013.com;gruu;opaque
Certificate name: voip12.tsdev-aastra.com

☑ Federate Presence

☑ Activate permanent subscriptions

LDAP filter: (telephoneNumber=*)

6.3.1 Prolog

The described method is based on the topic “Activating a UCMA 4.0 trusted application” (http://msdn.microsoft.com/en-us/library/office/dn466114.aspx) within the Microsoft Office development center.
These steps are necessary:

- Create a single application pool for every BluStar Server / DAL
- Create a trusted application for the application pool
- Create and import the required certificates
- Configure the Lync data source for the PresenceServer in the WebAdmin

All steps have to be performed with a domain administrator account.
Note: always use the fully qualified domain name (FQDN).

6.3.2 Create a Single Application Pool

The application pool has to be created on the Lync Server by using the “Topology Builder”.

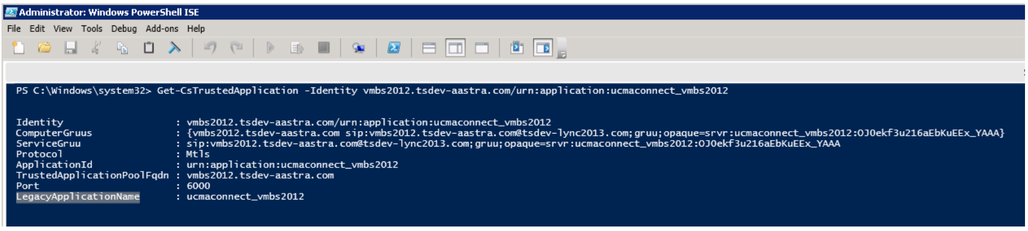
6.3.3 Create a Trusted Application

The trusted application will be created with the “Lync Server Management Shell”. Use “Run ISE as Administrator”.

- Note: the defined port, which will be used on the BluStar Server / DAL for the communication with the Lync server, needs to be accessible from the Lync Server
- Specify the FQDN of the application pool created one step before

With “Get-CsTrustedApplication” you get the necessary information for the Lync Data Source configuration of the Presence Server in the WebAdmin:

- LegacyApplicationName
- Port
- ServiceGruu - copy the whole line to <Application user agent uri (Gruu)> in the WebAdmin


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

```
PS C:\Windows\system32> Get-CsTrustedApplication -Identity vmbs2012.tsdev-aastra.com/urn:application:ucmaconnect_vmbs2012


Identity                    : vmbs2012.tsdev-aastra.com/urn:application:ucmaconnect_vmbs2012
ComputerGruus               : {vmbs2012.tsdev-aastra.com sip:vmbs2012.tsdev-aastra.com@tsdev-lync2013.com;gruu;opaque=srvr:ucmaconnect_vmbs2012:OJOekf3u216aEbKuEEx_YAAA}
ServiceGruu                 : sip:vmbs2012.tsdev-aastra.com@tsdev-lync2013.com;gruu;opaque=srvr:ucmaconnect_vmbs2012:OJOekf3u216aEbKuEEx_YAAA
Protocol                    : Mtls
ApplicationId               : urn:application:ucmaconnect_vmbs2012
TrustedApplicationPoolFqdn  : vmbs2012.tsdev-aastra.com
Port                        : 6000
LegacyApplicationName       : ucmaconnect_vmbs2012
```

6.3.4 Create and import the required certificates

Root certificate from the certificate authority (CA)
The root certificate exists on the server which acts as CA.
This root certificate has to be installed on the BluStar Server in the Local Computer store under “Trusted Root Certification Authorities”

Certificate for the BluStar Server
For the connection to the Lync Server, the DAL service needs a certificate to sign himself as a trusted server. This certificate has to be created with the “Lync Server Management Shell”. Use “Run ISE as Administrator”.

- Use Type = default
- Use ComputerFqdn = FQDN of the BluStar Server / DAL
- Define FriendlyName

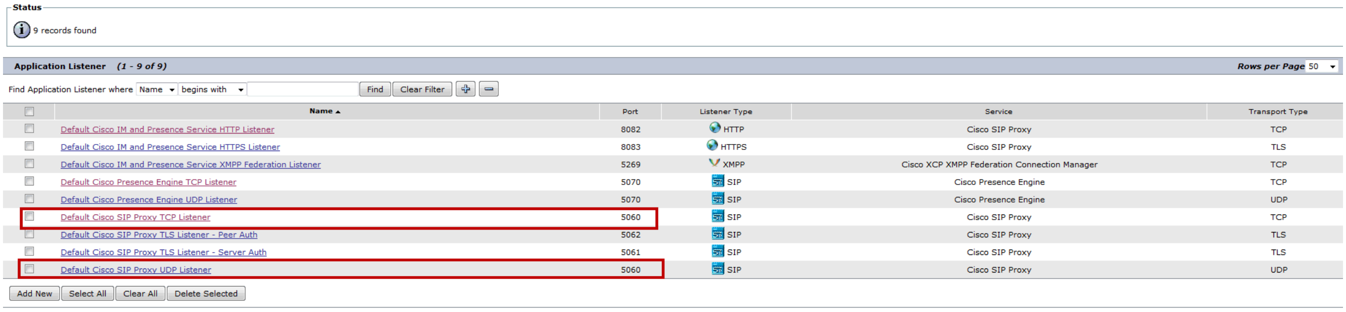
The value for “FriendlyName” is needed for the Lync Data Source configuration of the Presence Server in the WebAdmin.
Then export the certificate using mmc.

This certificate has to be installed on the BluStar Serve in the local Computer store under “Personal”.

6.4 Cisco Unified Presence Server (CUPS)

To prepare the CUPS Server for the BluStar Presence Server connection (use the "Cisco Unified CM IM and Presence Administration" web page and log in as admin):

1. Check the SIP Listener port on CUPS (System - Application Listeners) - Default is 5060



Status

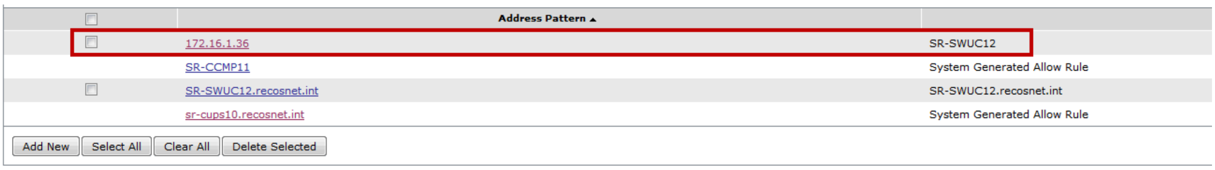
9 records found

Application Listener (1 - 9 of 9) Rows per Page 50

Find Application Listener where Name begins with [Find] [Clear Filter]

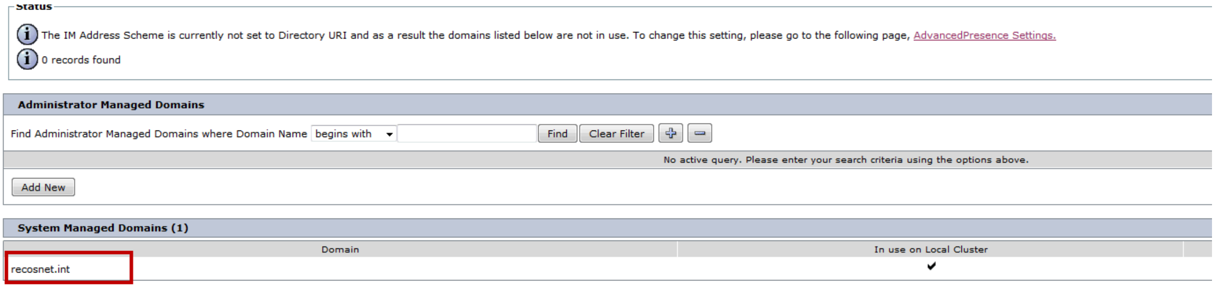
□	Name ▲	Port	Listener Type	Service	Transport Type
□	Default Cisco IM and Presence Service HTTP Listener	8082	HTTP	Cisco SIP Proxy	TCP
□	Default Cisco IM and Presence Service HTTPS Listener	8083	HTTPS	Cisco SIP Proxy	TLS
□	Default Cisco IM and Presence Service XMPP Federation Listener	5269	XMPP	Cisco XCP XMPP Federation Connection Manager	TCP
□	Default Cisco Presence Engine TCP Listener	5070	SIP	Cisco Presence Engine	TCP
□	Default Cisco Presence Engine UDP Listener	5070	SIP	Cisco Presence Engine	UDP
□	Default Cisco SIP Proxy TCP Listener	5060	SIP	Cisco SIP Proxy	TCP
□	Default Cisco SIP Proxy TLS Listener - Peer Auth	5062	SIP	Cisco SIP Proxy	TLS
□	Default Cisco SIP Proxy TLS Listener - Server Auth	5061	SIP	Cisco SIP Proxy	TLS
□	Default Cisco SIP Proxy UDP Listener	5060	SIP	Cisco SIP Proxy	UDP

2. Add the Presence Server's IP address to the incoming ACL (System - Security - Incoming ACL - Add New)



☐	Address Pattern ▲	
☐	172.16.1.36	SR-SWUC12
	SR-CCMP11	System Generated Allow Rule
☐	SR-SWUC12.recosnet.int	SR-SWUC12.recosnet.int
	sr-cups10.recosnet.int	System Generated Allow Rule

3. Check the SIP Domain of the CUPS Server (Presence - Domains)



Status

The IM Address Scheme is currently not set to Directory URI and as a result the domains listed below are not in use. To change this setting, please go to the following page, AdvancedPresence Settings.

0 records found

Administrator Managed Domains

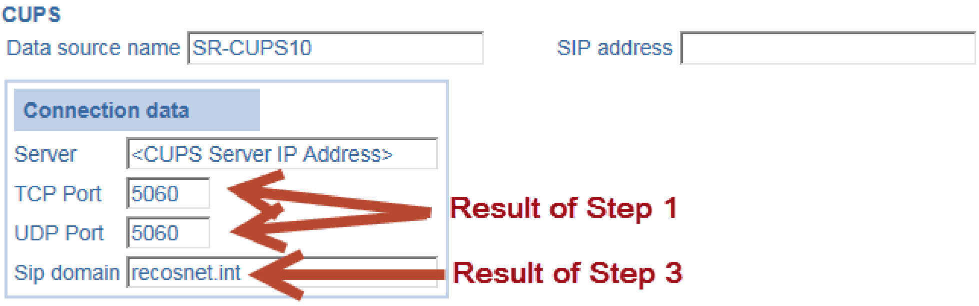
Find Administrator Managed Domains where Domain Name begins with

No active query. Please enter your search criteria using the options above.

System Managed Domains (1)

Domain	In use on Local Cluster
recosnet.int	✓

Then configure Server / Ports / SIP Domain accordingly in BluStar WebAdmin



CUPS

Data source name: SR-CUPS10

SIP address:

Connection data

Server: <CUPS Server IP Address>

TCP Port: 5060

UDP Port: 5060

Sip domain: recosnet.int

6.5 Troubleshooting Guide

6.5.1 Exchange 2007, 2010 and 2013

- To connect to Exchange 2007, Exchange 2010 or Exchange 2013 the WebService is used.
- WebService must be available on this server and the server must have enabled the role “CAS” (Client access Server).
- In a clustered NLB environment the connection is made to the virtual NLB name/IP-address and the traffic is routed to the available CAS server.

6.5.2 Check List

- Is the exchange user available?

  -> Try to request the WebService description with a browser like

  https://OUR_EXCHANGE_SERVER/EWS/exchange.asmx

  and use the login data for this user. If you get an error like “Error: Server not found” or “Error: Service not available” then you have not connected to the right host or the host does not contain the “Client-Access-Role”.

- Getting error “401”:

  Is “Basic Authentication” or “Windows Authentication” enabled at the virtual path “EWS“?

  Does the user have the needed rights?

  - Exchange Server 2007. Were the two needed commands executed in the Exchange Management Shell for Exchange 2007 Server?
  - Exchange Server 2010. Was the needed command executed in the Exchange Management Shell for Exchange 2010 Server?

- Presence connection or authentication fails:

  BluStar Server might not be in a domain or is in a different domain as the client resulting in failure of DNS name resolution. Of course, if DNS fails, you can always enter the IP address.

7 Application share

This feature does not require any configuration in BluStar Server.

- Only available on BluStar for PC client (Application share setup)
- Only available in a BluStar call
- Any BluStar device (iPad, iPhone, Mitel 8000i, BluStar for conference room) can “receive” an Application share session (of course, the remote systems must have the applicable hard- and software installed)

8 Advanced installation

8.1 Automated installation

This chapter describes how to avoid being prompted during the installation by leveraging configuration files for the setup procedure. Generic <setup.conf> files are provided with the BluStar Server; however, they require custom specific adjustment of most parameters (especially the default passwords used!). Using automated installation is only recommended for administrators who are experienced with the BluStar Server already.

8.1.1 Setup.conf

The installation of the BluStar server can be controlled with a configuration file. When a file with the name setup.conf is in the same directory as the setup.exe, then the parameters in the file are used for the installation instead of prompting the user.
If parameters are missing, or if no setup.conf – file is available, the required parameters have to be entered during the installation.
At the end of the installation, the BluStar Server will be active with a basic configuration.
More advanced configuration (e.g. the connection to a calendar system) has to be done after the installation with the Web Administration tool.
Here is an example of a setup.conf file:

```
################################################################################
#                                                                              #
#                         BLUSTAR SERVER 3.2                                   #
#                          SETUP PACKAGE                                       #
#                                                                              #
################################################################################

[Config]
################################################################################
#                                                                              #
# PBX CONFIGURATION                                                            #
# --------------------------------                                             #
#                                                                              #
# PBXType                  MX-ONE                                              #
#                          A400                                                #
#                          A5000                                               #
#                          NONE (BAS)                                          #
#                                                                              #
# PBXUser                  only needed for A400                                #
#                                                                              #
# PBXPassword              only needed for A400                                #
#                                                                              #
################################################################################
```

PBXType=A400 Defines the type of the used call manager.

PBXIP=192.165.103.48 IP address of the call manager.

PBXUser=csta MiVoice Office 400: user name that shall be used for connecting to the call manager.

PBXPassword=aastrapsw MiVoice Office 400: password of the user.

```
###############################################################################
#                                                                             #
# SQL CONFIGURATION                                                           #
# -------------------------------                                             #
#                                                                             #
# InstallSQL                 0 - use existing SQL Server                      #
#                            1 - install SQL Express                          #
#                                                                             #
# SQLServer                  only needed with InstallSQL=0                    #
#                                                                             #
# SQLUser                    only needed with InstallSQL=0                    #
#                                                                             #
# SQLPassword                password for <SQLUser> with InstallSQL=0         #
#                            password for user <sa> with InstallSQL=1         #
#                                                                             #
###############################################################################
```

InstallSQL=0 Defines whether a Microsoft SQL Express shall be installed or not.

SQLServer=VOIP12 Server name of an existing Microsoft SQL Server if no Microsoft SQL Express is installed.

SQLUser=sa Name of the user in the Microsoft SQL Server, only when an existing server is used.

SQLPassword=sqlpsw Password for the user in Microsoft SQL Server. When the Microsoft SQL Express is installed, then this password is used for the sa user. Please be aware the password has to fulfill the password requirements in the Microsoft Windows domain.

```
###############################################################################
#                                                                             #
# SETTINGS                                                                    #
# ---------------                                                             #
#                                                                             #
# InstallLdap                0 - no LDAP components will be installed         #
#                            1 - Aastra Directory Server and Administration   #
#                            will be installed                                #
#                                                                             #
# InstallTR87Interface                                                        #
#                            0 - no TR/87 Interface will be installed         #
#                            1 - Aastra TR/87 Interface                       #
#                            will be installed                                #
#                                                                             #
# TargetDir                  use special directory for the installation -     #
#                            default <%PROGRAMFILES%/Aastra/BluStar Server>   #
#                                                                             #
###############################################################################
```

InstallLdap=1 Defines whether the Aastra Directory Server has to be installed.

InstallTR87Interface=1 Defines whether the Aastra TR/87 Interface has to be installed.

TargetDir= Defines an installation path other than the default path.

```
#########################################################################
#                                                                       #
# GENERAL                                                               #
# --------------                                                        #
#                                                                       #
# Param          BLUSTAR - necessary startup parameter for              #
#                      the setup                                        #
#                                                                       #
# AllowDomain          0 - Server can't be member of a domain during    #
#                              the setup (due to domain policies)       #
#                      1 - Server can be member of a domain             #
#                                                                       #
#########################################################################
```

[Start]
Param=BLUSTAR

Can't be changed.

[Setup]
AllowDomain=1

Defines whether the server may be in a Microsoft Windows domain during the installation.

When the server is in a domain, the installation of Microsoft SQL Express may fail, if a password for the sa user is specified that doesn't meet the password complexity requirements of the domain.

The BluStar Server installation routine tries to apply changes to the IIS configuration to implement the webservices for the administration of the BluStar Server which may fail for similar reasons.

Recommended actions in such case:

- Revert the installation of the BluStar Server (see chapter 9 for details)
- install Microsoft SQL Express manually (start “SQLEXPR_2012_x64.exe”. provided in the “x64 directory of the BluStar Server installation package) and make sure the password for the SQL-admin “sa” entered during the installation is matches the password complexity requirements of the Windows Domain
- Install the BluStar Server but select the option to refer to an existing SQL server instead of installing the MS-SQL Express

8.2 Using an “external” MS-SQL database

To install the Aastra databases AastraConfig and AastraLog with another user than ‘sa’ the steps bellow are necessary. In the following example a new user ‘Aastra’ with the password ‘Aastra2013$’ is created. The steps can be performed in Enterprise Manager/Management Studio or by executing appropriate T-SQL statements via sqlcmd.

Step	Procedure
1	Prior to the installation of the databases create a SQL server login for the new user.
2	Give the new user dbcreator rights

Now the databases can be installed with the user ‘Aastra’. After installation of the databases the new user must get appropriate rights for the databases. AastraConfig should be made the default database for the new user

3	As ‘sa’ execute the following comands: USE master ALTER AUTHORIZATION ON DATABASE::AastraConfig TO Aastra ALTER AUTHORIZATION ON DATABASE::AastraLog TO Aastra

If you don’t have a local database system installation the setup will also create the databases remotely.

Important
For data redundancy using a backup Microsoft SQL server, please use a Microsoft SQL cluster solution.

8.3 Using non default database names

When running the BluStar Server databases in large Microsoft SQL Server environments the default database names of the databases used by the BluStar Server can be renamed for special purposes (like having more than one database located in a Microsoft SQL Server Cluster). The following chapters briefly describe the handling and the limitations; nevertheless the DB administrator must be aware that specific SQL knowledge is required for such adjustments.

8.3.1 Changing the database names

The renaming of the database has to be done by the customer’s DB administrator.
Also possible is the initial installation of the database using a database restore and the new name.
The new database name has then to be entered for the access of the different BluStar Server services. This can be done using the tool “DALConfigurationTool.exe” which was installed to the BluStar Server directory. The new name can there be entered and – after confirming the new name – it will be saved to the registry (HKLM/Software/Aastra/DAL/DB).
A restart of all BluStar Server related services is necessary.

8.3.2 Restrictions using non-default database names – no automated backup

The internal backup and restore features of the BluStar Server system won't work using non-default database names. Therefore in the web administration of the BluStar Server the menu option "Tools/Database backup" will be invisible when using non default database names.
In this case the DB administrator must take care for making backups like on every SQL database.

8.3.3 Updating databases

When using non default database names the installation of service packs and updates has to be done manually by the customer's DB administrator.
For installation of a new service pack adapted SQL scripts are provided to update the databases. Mentioned SQL scripts require the "non-default name" of the database to be entered in the first line (scripts must be edited before use). Afterwards these scripts have to be run on the SQL Server (e.g. using a command line tool like sqlcmd.exe).

9 Remove BluStar Server installation

This section will address the uninstall procedure and describe the necessary steps to remove the BluStar Server application and all related services from the system.

9.1 Overview

Step	Procedure
1	Stop all running Aastra services in the Windows service manager
2	Uninstall BluStar Server
3	Uninstall Microsoft SQL 2012 Express (optional)
4	Reboot the server

9.2 Step 1 – Stop all running Aastra services

Start Windows Services Manager and stop all services beginning with “Aastra”.
Additionally, stop the IIS Admin Service, if available.

9.3 Step 2 – Uninstall BluStar Server

On the server where the CTI Server is installed, start Windows Control Panel and enter “Add or Remove Programs”. In the dialog that appears find BluStar Server, choose the Remove option and follow the instructions.
The CTI Server is a part of the BluStar Server installation setup.

9.4 Step 3 – Uninstall Microsoft SQL 2012 Express (optional)

Microsoft’s SQL 2012 Express server is a part of the BluStar Server install. The SQL server will not be uninstalled with the BluStar Server uninstall procedure because it may host other applications data, too. There is an option for the Microsoft SQL server in the “Add or Remove Programs” panel called Microsoft SQL Server 2012. Choose the Remove Option and follow the instructions.

9.5 Step 4 – Check if all directories were removed

The un-installation of the components listed above may leave directories and files behind which may cause trouble when installing the BluStar Server again on the same machine (i.e. database files not belonging to the BluStar Server).
Please verify that the directories are removed during the un-installation procedure.

9.6 Step 4 – Reboot the server

After you rebooted the server, removing of BluStar Server is completed.

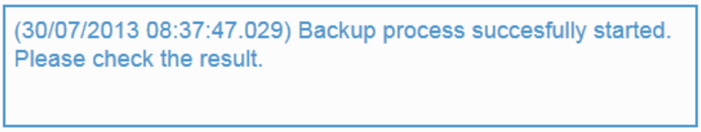
10 Backup, restore, database relocation / name change

10.1 Backing up the BluStar Server's database "AastraConfig"

Menu: Tools → Database → Backup and Restore, section "Backup"
The BluStar Server can create automated backups of its database during normal operation but the admin may initiate an immediate backup, too.
To activate the automated backup

- the option "Database backup active" must be selected
- the filename and path for the backup-file(s) must be provided
- the time of the day for initiating the automated regular backup must be provided (hh:mm)
- by default the BluStar Server keeps 2 generations of backup files ("Number of files")

The backup file created contains the SQL data bases "AastraConfig.mdf" and its transaction file "AastraConfig.ldf".
For creating an immediate backup the favored path and file name must be provided in the section "Start configuration backup immediately". Once the "Start backup" button is clicked the backup will be created instantaneously; the upper right corner of the web-gui will show a message like



(30/07/2013 08:37:47.029) Backup process succesfully started. Please check the result.

For verifying the result, please check if the file was successfully created and the file size is > 0 bytes.

10.2 Restoring system database "AastraConfig"

Menu: Tools → Database → Backup and Restore, section "Restore"
To restore a database from a database backup the following steps must be performed:

- Select the favored backup file from the drop down box
- Load the selected database temporarily by clicking on the "Read" button.
  The backup database will be restored to a temporary database allowing the selection of the part of the database to be restored.
- Selection of the type of restore (complete database, links) and the favored parts of the database backup from the list box.
  Please note: It is strongly recommended to restore the "Entire database" only to avoid inconsistencies.
- After clicking the "Restore data" button the restore will be initiated.
  Dependent on the size of the database the restore action may take some seconds to be complete. Once restored, the database will be used instantaneously for the operation of the BluStar Server.

10.3 Database relocation / name change

Menu: Tools → Database → Rename server
It is possible to rename the BluStar Server the database belongs to (for advanced installations: all BluStar Servers, too). This may be useful when the BluStar Server installation has been moved to another server hardware.
Select the current name of the BluStar server(s) from the drop down list and provide the new name. After clicking the Rename button all Aastra Servers with the selected old name in the table <ServerData> will be renamed and all references in the database are adapted.
Please note that the operation described will change the name of the BluStar Server(s) in the database currently used; thus backing up the database before initiation the “Rename server” action is strongly recommended.

Mitel
Powering connections

mitel.com